SIFAT POLINOMIAL PERMUTASI PADA MODULO PRIMA BERPANGKAT (p^n)

SKRIPSI

Oleh:
QOSIMIL JUNAIDI
NIM. 09610102

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2014

SIFAT POLINOMIAL PERMUTASI PADA MODULO PRIMA BERPANGKAT (p^n)

SKRIPSI

Diajukan Kepada:
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Sains (S.Si)

Oleh:
QOSIMIL JUNAIDI
NIM. 09610102

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2014

SIFAT POLINOMIAL PERMUTASI PADA MODULO PRIMA BERPANGKAT (p^n)

SKRIPSI

Oleh:
QOSIMIL JUNAIDI
NIM. 09610102

Telah Diperiksa dan Disetujui untuk Diuji:
Tanggal: 12 Desember 2013

Pembimbing I,	Pembimbing II,
H. Wahyu H. Irawan, M.Pd	Ach. Nashichuddin, M.A
NIP. 1971 0420 200003 1 003	NIP. 1973 0705 200003 1 002

Mengetahui,
A.n. Ketua Jurusan Matematika
Sekretaris Jurusan Matematika

Fachrur Rozi, M.Si
NIP. 19800527 200801 1 012

SIFAT POLINOMIAL PERMUTASI PADA MODULO PRIMA BERPANGKAT (p^n)

SKRIPSI

Oleh:
QOSIMIL JUNAIDI
NIM. 09610102

Telah Dipertahankan di Depan Dewan Penguji Skripsi dan
Dinyatakan Diterima Sebagai Salah Satu Persyaratan untuk
Memperoleh Gelar Sarjana Sains (S.Si)
Tanggal: 10 Januari 2014

Penguji Utama	: Hairur Rahman, M.Si NIP. 19800429 200604 1 003	_____
Ketua Penguji	: Drs. H. Turmudi, M.Si NIP. 19571005 198203 1 006	_____
Sekretaris Penguji	: H. Wahyu H. Irawan, M.Pd NIP. 1971 0420 200003 1 003	_____
Anggota Penguji	: Ach. Nashichuddin, M.A NIP. 1973 0705 200003 1 002	_____

Mengesahkan,
A.n. Ketua Jurusan Matematika
Sekretaris Jurusan Matematika

Fachrur Rozi, M.Si
NIP. 19800527 200801 1 012

PERNYATAAN KEASLIAN TULISAN

Saya yang bertandatangan di bawah ini:

Nama	:	Qosimil Junaidi
NIM	:	09610102
Jurusan	:	Matematika
Fakultas	:	Sains dan Teknologi

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar hasil karya saya sendiri, bukan pengambilalihan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 6 Februari 2014

Yang membuat pernyataan,

Qosimil Junaidi

NIM. 09610102

MOTTO

Milikmu hanya hari ini karena kemarin adalah masa yang telah berlalu dan besok adalah masa yang semu...

PERSEMBAHAN

Dengan mengucap rasa syukur kepada Allah Yang Maha Pengasih dan Maha Penyayang atas segala limpahan rahmat, taufik, dan hidayah-Nya yang selalu diberikan kepada penulis sehingga penulis dapat menyelesaikan skripsi ini.

Dengan segala kerendahan hati skripsi ini penulis persembahkan kepada orang tua tercinta,
Ayahanda Buchori dan Ibunda Siti Kulsum,
yang telah mengorbankan seluruh hidupnya untuk penulis.

Kepada adik tercinta Maisyaroh dan Mas'udi
atas dukungan dan do'anya.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Syukur *alhamdulillah* penulis ucapkan ke hadirat Allah SWT, Tuhan semesta alam yang telah melimpahkan rahmat, taufik, hidayah-Nya, sehingga penulis dapat menyelesaikan studi di Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang sekaligus menyelesaikan skripsi ini dengan baik.

Keberhasilan penulisan skripsi ini tidak lepas dari bantuan, arahan dan bimbingan dari berbagai pihak, baik berupa pikiran, motivasi, tenaga, ataupun doa dan restu. Karena itu penulis mengucapkan terima kasih kepada:

1. Prof. Dr. H. Mudjia Rahardjo, M.Si, selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. drh. Hj. Bayyinatul Muchtaromah, M.Si, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Abdussakir, M.Pd, selaku Ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Hairur Rahman, M.Si, selaku dosen wali yang telah membimbing dan memberi arahan dari semester awal hingga akhir.
5. H. Wahyu H. Irawan, M.Pd, selaku dosen pembimbing skripsi yang dengan sabar telah meluangkan waktu memberikan bimbingan dan arahan dalam penyelesaian skripsi ini.

6. Ach. Nashichuddin, M.A, selaku dosen pembimbing keagamaan yang telah memberikan banyak arahan dan bimbingan dalam penyelesaian skripsi ini.
7. Ayah, Ibu, Adik, dan seluruh keluarga tercinta yang selalu memberikan motivasi dan doa tanpa kenal lelah bagi penulis untuk selalu konsisten dalam bersungguh-sungguh meraih cita-cita.
8. Segenap sivitas akademika Jurusan Matematika, terutama seluruh dosen, terima kasih atas segenap ilmu dan bimbingannya.
9. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang turut mendukung kelancaran penyempurnaan skripsi ini.

Semoga skripsi ini dapat memberikan manfaat kepada para pembaca khususnya bagi penulis secara pribadi. *Amin Ya Rabbal Alamin*.

Wassalamu'alaikum Wr. Wb.

Malang, Februari 2014

Penulis

DAFTAR ISI

ABSTRAK

Junaidi, Qosimil. 2014. **Sifat Polinomial Permutasi pada Modulo Prima Berpangkat** (p^n). Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
Pembimbing: (I) H. Wahyu H. Irawan, M.Pd
(II) Ach. Nashichuddin, M.A

Kata Kunci: Polinom, Permutasi, dan Modulo.

Polinom $f(x)=\sum_{i=0}^{\infty} a_i x^i$ dengan a_0 ring R adalah polinomial permutasi jika ada himpunan berhingga (A) sedemikian hingga $f: A \to A$ dan f bersifat satu-satu dan onto. Polinom yang digunakan dalam penelitian ini adalah $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0, a_1, \ldots, a_d \in \mathbb{Z}$.

Penelitian ini bertujuan untuk mengetahui bagaimana sifat atau ciri-ciri dari koefisien pada suatu polinom yang mempermutasikan modulo p^n. Kemudian hasil penelitian ini adalah sifat Polinomial Permutasi (PP) pada:

1. $M_2 \Leftrightarrow (a_1+a_2+\cdots+a_d)$ ganjil.
2. $M_2^n \Leftrightarrow a_1$ ganjil, $(a_2+a_4+a_6+\cdots+a_d)$ dan $(a_3+a_5+a_7+\cdots+a_{d-1})$ genap.
3. $M_3 \Leftrightarrow (a_1+a_3+a_5+\cdots) \not\equiv 0 \pmod 3$ dan $(a_2+a_4+a_6+\cdots) \equiv 0 \pmod 3$.
4. $M_3^n \Leftrightarrow a_1 \not\equiv 0 \pmod 3$, $(a_1+a_3+a_5+\cdots) \not\equiv 0 \pmod 3$, $(a_2+a_4+\ldots+a_d) \equiv 0 \pmod 3$, $T[1]+U[2] \not\equiv 0 \pmod 3$, dan $M[1]+N[2] \not\equiv 0 \pmod 3$.
5. $M_5 \Leftrightarrow (a_2+a_6+\cdots+a_{d-2})^2 \equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$ dan $(a_4+a_8+\cdots+a_d) \equiv 0 \pmod 5$, $\forall d=4m,\ m \geq 1$.
6. $M_5^n \Leftrightarrow \forall d=4m,\ m \geq 1$ maka:
   a. $a_1 \not\equiv 0 \pmod 5$
   b. $(a_4+a_8+a_{12}+\cdots+a_d) \equiv 0 \pmod 5$,
   c. $(a_2+a_6+\cdots+a_{d-2})^2 \equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$,
   d. $A[1]+B[2]+C[3]+D[4] \not\equiv 0 \pmod 5$,
   e. $E[1]+F[2]+G[3]+H[4] \not\equiv 0 \pmod 5$,
   f. $I[1]+J[2]+K[3]+L[4] \not\equiv 0 \pmod 5$,
   g. $P[1]+Q[2]+R[3]+S[4] \not\equiv 0 \pmod 5$.

ABSTRACT

Junaidi, Qosimil. 2014. **Properties of Permutation Polynomials Modulo a Prime-Power** $\left(p^n\right)$. Thesis. Department of Mathematics Faculty of Science and Technology The State Islamic University Maulana Malik Ibrahim Malang.
Promotor: (I) H. Wahyu H. Irawan, M.Pd
(II) Ach. Nashichuddin, M.A

Keywords: Polynomial, Permutation, and Modulo.

Polynomial $f(x)=\sum_{i=0}^{\infty} a_i x^i$ with $a_i \in$ ring R is permutation polynomials if there is finite set (A) such that $f: A \to A$ and f are one-one and onto. This research use polynomial $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ with $a_0, a_1, \ldots, a_d \in \mathbb{Z}$.

The purpose of this research to understand properties or characteristic coefficient in a polynomial that permutes modulo p^n. Then result of this research is properties of Permutation Polynomials (PP) on:

1. $M_2 \Leftrightarrow (a_1+a_2+\ldots+a_d)$ is odd.
2. $M_2^n \Leftrightarrow a_1$ is odd, $(a_2+a_4+a_6+\ldots+a_d)$ and $(a_3+a_5+a_7+\ldots+a_{d-1})$ even.
3. $M_3 \Leftrightarrow (a_1+a_3+a_5+\cdots) \not\equiv 0 \pmod 3$ and $(a_2+a_4+a_6+\cdots) \equiv 0 \pmod 3$.
4. $M_3^n \Leftrightarrow a_1 \not\equiv 0 \pmod 3$, $(a_1+a_3+a_5+\cdots) \not\equiv 0 \pmod 3$, $(a_2+a_4+a_6+\cdots) \equiv 0 \pmod 3$, $T[1]+U[2] \not\equiv 0 \pmod 3$, and $M[1]+N[2] \not\equiv 0 \pmod 3$.
5. $M_5 \Leftrightarrow (a_2+a_6+\cdots+a_{d-2})^2 \equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$ and $(a_4+a_8+\ldots+a_d) \equiv 0 \pmod 5$, $\forall d=4m,\ m \geq 1$.
6. $M_5^n \Leftrightarrow \forall d=4m,\ m \geq 1$ then:
   a. $a_1 \not\equiv 0 \pmod 5$
   b. $(a_4+a_8+a_{12}+\cdots+a_d) \equiv 0 \pmod 5$,
   c. $(a_2+a_6+\cdots+a_{d-2})^2 \equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$,
   d. $A[1]+B[2]+C[3]+D[4] \not\equiv 0 \pmod 5$,
   e. $E[1]+F[2]+G[3]+H[4] \not\equiv 0 \pmod 5$,
   f. $I[1]+J[2]+K[3]+L[4] \not\equiv 0 \pmod 5$,
   g. $P[1]+Q[2]+R[3]+S[4] \not\equiv 0 \pmod 5$.

الملخص

الجنيد, قاسم. ٢٠١٤. **طبيعه التقليب متعدد الحدود مرتبة رئيس** . قسم الرياضيات, كلية العلوم والتكنولوجي,
جامعة مولانا مالك ابراهيم الاسلا مية الحكومية بمالانج.
المستشار : (١) الحج وحيو هنكي اراوان, المجستير
(٢) احمد نصيح الدين, المجستير

الكلمات الر ئيسية: متعدد الحدود, التباديل, ونمطية.

متعدد الحدود $f(x)=\sum_{i=0}^{\infty} a_i x^i$ مع $a_i \in R$ هو متعدد الحدود التقليب إذا كان هناكمجموعات محدودة (A) بحيث جمعه $f: A \to A$ و f هوواحد وواحدوعلى. متعدد الحدود المستخدمة في هذه الدرسة هو $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ مع $a_0, a_1, \ldots, a_d \in \mathbb{Z}$.

تهدف هذه الدرسات الى تحديد مدى طبيعة أو خصائص المعاملات في كاثيرات الحودود التي تباديل نمطيه (p^n) ثم النتائج هذه الدرسة هي طبيعة التقليب متعدد الحدود (PP) في:

١. $M_2 \Leftrightarrow (a_1+a_2+\ldots+a_d)$ غريب.

٢. $M_2{}^n \Leftrightarrow (a_1+a_2+\ldots+a_d)$ غريب, $(a_2+a_4+a_6+\ldots+a_d)$ و $(a_3+a_5+a_7+\ldots+a_{d-1})$ حتي.

٣. $M_3 \Leftrightarrow (a_1+a_3+a_5+\cdots) \not\equiv 0 \pmod 3$ و $(a_2+a_4+a_6+\cdots)\equiv 0 \pmod 3$.

٤. $M_3{}^n \Leftrightarrow a_1 \not\equiv 0 \pmod 3$, $(a_1+a_3+a_5+\cdots)\not\equiv 0 \pmod 3$, $(a_2+a_4+a_6+\cdots)$, $0 \pmod 3 \equiv$ $T[1]+U[2]\not\equiv 0 \pmod 3$ و $M[1]+N[2]\not\equiv 0 \pmod 3$.

٥. $M_5 \Leftrightarrow \forall d=4m,\ m\geq 1$ $(a_4+a_8+\cdots+a_d)\equiv 0 \pmod 5$ و $(a_2+a_6+\cdots+a_{d-2})^2 \equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$.

٦. $M_5{}^n \Leftrightarrow \forall d=4m,\ m\geq 1$:

أ. $a_1 \not\equiv 0 \pmod 5$

ب. $(a_4+a_8+a_{12}+\cdots+a_d)\equiv 0 \pmod 5$

ت. $(a_2+a_6+\cdots+a_{d-2})^2 \equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$

ث. $A[1]+B[2]+C[3]+D[4]\not\equiv 0 \pmod 5$

ج. $E[1]+F[2]+G[3]+H[4]\not\equiv 0 \pmod 5$

ح. $I[1]+J[2]+K[3]+L[4]\not\equiv 0 \pmod 5$

خ. $P[1]+Q[2]+R[3]+S[4]\not\equiv 0 \pmod 5$

BAB I

PENDAHULUAN

1.1 Latar Belakang

Alam semesta memuat bentuk-bentuk dan konsep matematika, meskipun alam semesta tercipta sebelum matematika itu ada. Alam semesta serta segala isinya diciptakan Allah dengan ukuran-ukuran yang cermat dan teliti, dengan perhitungan-perhitungan yang mapan, dan dengan rumus-rumus serta persamaan yang seimbang dan rapi. Semua yang ada di alam ini ada ukurannya, ada hitungan-hitungannya, ada rumusnya, atau ada persamaannya. Namun rumus-rumus yang ada sekarang bukan diciptakan manusia sendiri, tetapi sudah disediakan. Manusia hanya menemukan dan menyimbolkan dalam bahasa matematika (Abdussakir, 2007:79-80). Hal ini sesuai dengan Firman Allah dalam Surat Al-Furqan ayat 2 yang berbunyi:

...وَخَلَقَ كُلَّ شَيْءٍ فَقَدَّرَهُۥ تَقْدِيرًا

"...Dia telah menciptakan segala sesuatu, dan Dia menetapkan ukuran-ukurannya dengan serapi-rapinya".

Aljabar sebagai salah satu bagian ilmu matematika memiliki cabang yaitu aljabar abstrak dan aljabar linier. Aljabar abstrak atau yang sekarang lebih dikenal dengan struktur aljabar mempunyai banyak materi yang dibahas dan dikembangkan. Materi yang dibahas pada struktur aljabar pada dasarnya tentang himpunan dan operasinya. Sehingga ketika mempelajarinya, selalu berhubungan dengan himpunan (yang tak kosong) yang anggota-anggotannya dapat

dioperasikan dengan satu atau lebih operasi biner. Himpunan dengan satu operasi biner dan memenuhi beberapa sifat tertentu disebut grup. Sedangkan himpunan yang melibatkan dua operasi biner serta memenuhi beberapa sifat tertentu disebut ring. Masing-masing dari grup dan ring dikembangankan dengan banyak sifat dan syarat tertentu menjadikan grup dan ring semakin kompleks. Polinom dan permutasi merupakan perkembangan dari pembahasan mengenai teori grup dan ring.

Polinom atau suku banyak merupakan deret dengan bentuk $f(x)=\sum_{i=0}^{\infty} a_i x^i$ dengan a_i merupakan unsur dari sebuah ring *R* dan *x* variabel bebas. Sedangkan, permutasi adalah pemetaan satu-satu dari himpunan berhingga pada himpunan itu sendirinya (Raisinghania dan Anggarwal, 1980:115). Sehingga jika polinom $f(x)$ memetakan himpunan berhingga *A* kembali ke himpunan A itu sendiri maka polinom $f(x)$ disebut polinomial permutasi atau $f(x)$ polinom yang mempermutasikan himpunan A. Oleh sebab itu, dalam penelitian kali ini penulis tertarik untuk mengkaji tentang sifat polinomial permutasi pada modulo prima berpangkat **(** p^n **)**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan sebelumnya, maka penulis akan membahas tentang polinomial permutasi pada modulo prima berpangkat (p^n). Sehingga, rumusan masalah dalam skripsi ini adalah bagaimana sifat polinomial permutasi pada modulo prima berpangkat (p^n)?

1.3 Batasan Masalah

Ruang lingkup kajian aljabar dalam matematika sangat luas. Agar tidak melampaui tujuan dari penulisan skripsi ini maka dibutuhkan suatu batasan masalah yang dapat dijadikan acuan dalam penulisan lebih lanjut. Masalah yang akan dibahas oleh peneliti adalah sifat polinomial permutasi pada modulo prima berpangkat $\left(p^n\right)$. Batasan dari penelitian ini ada dua hal. Pertama, sifat yang akan diteliti berkaitan dengan koefisien-koefisien pada polinom yang digunakan. Kedua, modulo yang digunakan adalah modulo 2^n, 3^n, dan 5^n dengan $n \in \mathbb{Z}^+$.

1.4 Tujuan Penelitian

Sesuai dengan latar belakang dan rumusan masalah, maka tujuan pembahasan skripsi ini adalah untuk mengetahui bagaimana sifat polinomial permutasi pada modulo prima berpangkat $\left(p^n\right)$.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini sebagai berikut:

1. Memberikan informasi mengenai sifat polinomial permutasi sehingga dapat menjadi acuan peneliti lain untuk menentukan sifat polinomial permutasi dengan modulo yang berbeda atau menggunakan polinom yang lain yang belum dikaji dalam penelitian ini.
2. Hasil penelitian ini dapat digunakan sebagai tambahan kepustakaan yang dijadikan sarana pengembangan wawasan keilmuan khususnya di jurusan matematika untuk mata kuliah aljabar atau teori bilangan.

1.6 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode penelitian kepustakaan, yaitu dengan mengkaji buku, jurnal, dan literatur lain yang mendukung penelitian ini. Adapun langkah-langkah penelitian yang digunakan sebagai berikut:

1. Diberikan polinom $f(x)$.
2. Memberikan contoh Polinomial Permutasi (PP) pada modulo prima berpangkat (p^n) sesuai dengan definisi PP yang ada.
3. Menentukan sifat atau ciri PP pada modulo 2, 3 dan 5.
4. Menetukan sifat PP pada modulo 2^n, 3^n, dan 5^n dengan $n>1$.
5. Memberikan kesimpulan dari hasil penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan penulis pada tugas akhir (skripsi) ini tersusun atas empat bab, diantaranya:

Bab I Pendahuluan

Bab ini terdiri latar belakang permasalahan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

Bab II Kajian Pustaka

Bab ini berisi teori-teori yang menjadi acuan dari penelitian ini. Adapun teori-teori tersebut adalah fungsi, kongruensi, modulo, polinom, permutasi serta beberapa konsep agama yang berhubungan pembahasan.

Bab III Pembahasan

Bab ini berisi hasil penelitian tentang sifat polinomial permutasi pada modulo prima berpangkat.

Bab IV Penutup

Bab ini memaparkan kesimpulan dari penelitian dan saran untuk penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1 Fungsi

Fungsi atau disebut juga pemetaan adalah pemasangan tepat satu unsur dari dua himpunan. Misalnya pemetaan (pemasangan) antara himpunan "seluruh mahasiswa matematika" dan himpunan "seluruh orang tua atau wali mahasiswa", maka masing-masing mahasiswa akan memiliki tepat satu pasangan dari himpunan orang tua tersebut. Lebih jelasnya diberikan dua definisi dibawah ini, yaitu:

Definisi 2.1.1

Misalkan X dan Y dua himpunan tak kosong, maka fungsi atau pemetaan dari X ke Y adalah pemasangan satu unsur $x \in X$ dengan tepat satu unsur di Y yang dinotasikan dengan $f(x)$ atau $f : X \to Y$ (Raisinghania dan Anggarwal, 1980:14).

Definisi 2.1.2

Fungsi $f : X \to Y$ dikatakan **fungsi satu-satu (injektif)** jika dan hanya jika $f(x) = f(y) \Rightarrow x = y \quad \forall x \in X, \; y \in$. Fungsi $f : X \to Y$ dikatakan **fungsi onto (surjektif)** jika dan hanya jika $f(X) = Y$. Fungsi $I : X \to X$ adalah **fungsi identitas**, di mana $I(x) = x, \quad \forall x \in X$ (Raisinghania dan Anggarwal, 1980:14-15).

2.2 Kongruensi dan Modulo

Definisi kongruensi adalah sebagai berikut:

Definisi 2.2.3

Misalkan untuk sebarang bilangan bulat a, b dan bilangan bulat positif n. Maka a kongruen dengan b pada modulo n, dan di tulis $a \equiv b \pmod{n}$, jika beda atau sisa dari $(a-b)$ adalah kelipatan dari n atau $a = b + kn (k \in \mathbb{Z})$ (Lidl dan Neiderreiter, 1997:4).

Dari definisi di atas diperoleh untuk sebarang $k \in \mathbb{Z}$ maka dapat dibentuk kelas ekuivalensi yang dilambangkan dengan $[a]$ yaitu kelas kongruensi atau kelas sisa dari $(a \bmod n)$ dan terdiri dari bilangan bulat yang berbeda dari a sesuai dengan kelipatan dari n. Kelas tersebut adalah

$$[a] = \{a + kn \mid k \in \mathbb{Z}\}$$
$$= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

Selanjutnya kelas ekuivalensi akan disebut "kongruensi modulo". Kemudian apabila himpunan $\mathbb{Z}$ dipartisi sesuai dengan kongruensi modulo n maka akan membentuk kelas-kelas dibawah ini:

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\},$$
$$[1] = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\},$$
$$[2] = \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\},$$
$$\vdots$$
$$[n-1] = \{\ldots, -2n-1, -n-1, -1, n-1, 2n-1, \ldots\}.$$

Sehingga diperoleh himpunan kelas sisa modulo n atau biasanya disebut modulo n saja, yaitu:

$\mathbb{Z}_n = \{[0],[1],[2],\ldots,[n-1]\}$ (Lidl dan Neiderreiter, 1997:4).

Selanjutnya, pada $\mathbb{Z}_n$ akan dikenakan operasi penjumlahan dan perkalian yang tentunya berbeda dengan penjumlahan dan perkalian pada bilangan bulat. Menurut Raisinghania dan Anggarwal (1980), jumlah dua kelas sisa $[a]$ dan $[b]$ dengan $a,b \in \mathbb{Z}$ adalah

$$[a]+[b]=[a+b], \forall a,b \in \mathbb{Z}.$$

Buktinya, misalkan $a,b,c,d \in \mathbb{Z}$ sedemikian hingga $[a]=[c]$ dan $[b]=[d]$ maka

$[a]=[c]$ dan $[b]=[d] \Rightarrow a \equiv c \pmod{n}$ dan $b \equiv d \pmod{n}$

$\Rightarrow (a-c)$ dapat dibagi n dan $(b-d)$ dapat dibagi n

$\Rightarrow (a-c)+(b-d)$ dapat dibagi n

$\Rightarrow (a+b)-(c+d)$ dapat dibagi n

$\Rightarrow (a+b) \equiv (c+d) \pmod{n}$

$\Rightarrow [a+b]=[c+d]$

$\Rightarrow [a]+[b]=[c]+[d].$

Lalu, menurut Raisinghania dan Anggarwal (1980), perkalian dua kelas sisa $[a]$ dan $[b]$ dengan $a,b \in \mathbb{Z}$ adalah

$$[a][b]=[ab], \forall a,b \in \mathbb{Z}.$$

Buktinya, misalkan $a,b,c,d \in \mathbb{Z}$ sedemikian hingga $[a]=[c]$ dan $[b]=[d]$ maka

$[a]=[c]$ dan $[b]=[d] \Rightarrow a \equiv c \pmod{n}$ dan $b \equiv d \pmod{n}$

$\Rightarrow (a-c)$ dapat dibagi n dan $(b-d)$ dapat dibagi n

$\Rightarrow b(a-c)$ dapat dibagi n dan $c(b-d)$ dapat dibagi n

$\Rightarrow b(a-c)+c(b-d)$ dapat dibagi n

$\Rightarrow (ab+bc)-(bc+cd)$ dapat dibagi n

$\Rightarrow (ab-cd)$ dapat dibagi n

$\Rightarrow ab \equiv cd \pmod{n}$

$\Rightarrow [ab]=[cd]$

$\Rightarrow [a][b]=[c][d]$.

Contoh 2.1

Diberikan himpunan bilangan bulat $(\mathbb{Z})$, kemudian partisi menjadi 5 sehingga diperoleh modulo 5 atau $\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$ dengan:

$[0]=\{\ldots,-10,-5,0,5,10,\ldots\}$

$[1]=\{\ldots,-9,-4,1,6,11,\ldots\}$

$[2]=\{\ldots,-8,-3,2,7,12,\ldots\}$

$[3]=\{\ldots,-7,-2,3,8,13,\ldots\}$

$[4]=\{\ldots,-6,-1,1,9,14,\ldots\}$

Kemudian operasikan setiap unsur di $\mathbb{Z}_5$ dengan operasi penjumlahan dan perkalian, sehingga diperoleh:

1. Penjumlahan pada $\mathbb{Z}_5$

   Ambil $[a_1]=[0]$ dan $[a_2]=[1]$ maka

   $[a_1]+[a_2]=[0]+[1]=[0+1]=[1]$

   Dengan cara yang sama diperoleh hasil penjumlahan dari masing-masing unsur pada $\mathbb{Z}_5$ yaitu dengan tabel berikut:

   Tabel 2.1. Penjumlahan Kelas Sisa Modulo 5 ($\mathbb{Z}_5$)

$+_5$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

   Keterangan: $+_5$ menunjukkan operasi penumlahan pada $\mathbb{Z}_5$.

2. Perkalian pada $\mathbb{Z}_5$

   Ambil $[a_1]=[0]$ dan $[a_2]=[1]$ maka

   $[a_1][a_2]=[0][1]=[0\cdot 1]=[0].$

   Dengan cara yang sama diperoleh hasil perkalian dari masing-masing unsur pada $\mathbb{Z}_5$ yaitu dengan tabel berikut:

Tabel 2.2. Perkalian Kelas Sisa Modulo 5 ($\mathbb{Z}_5$)

$\times_5$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Keterangan: $\times_5$ menunjukkan operasi perkalian pada $\mathbb{Z}_5$.

2.3 Grup

Definisi 2.3.1

Himpunan tak kosong *G* dengan operasi biner + yang tertutup di *G* yang disimbolkan (*G*, +) disebut **grup** jika memenuhi:

1. Sifat asosiatif

   $$a + (b + c) = (a + b) + c\,(\forall a,b \in G).$$

2. Ada unsur identitas (*i*).
3. $i + a = a + i = a \;\; (\forall a, i \in G)$.
4. Masing-masing unsur *G* memiliki invers

   $a + a^{-1} = a^{-1} + a = i \;\; (\forall a, a^{-1} \in G)$ (Raisinghania dan Anggarwal, 1980:31).

Definisi 2.3.2

Grup (*G*, +) adalah **grup abel** atau **grup komutatif** jika dan hanya jika operasi + bersifat komutatif $(a + b = b + a, \; \forall a,b \in G)$(Raisinghania dan Anggarwal, 1980:31).

Untuk penyederhanaan penulisan maka (*G*, +) akan ditulis *G*.

Sesuai definisi 2.3.1 maka $(\mathbb{Z}_5, +_5)$ adalah grup karena memenuhi persyaratan untuk menjadi grup yaitu tertutup, asosiatif, ada identitas, dan masing-masing unsur memiliki invers. Sedangkan $(\mathbb{Z}_5, \times_5)$ bukan grup karena jika $[0]$ identitas maka hanya $[0]$ yang memiliki invers.

2.4 Ring (Gelanggang)

Subbab ini menjelaskan pengertian ring dan macam-macamnya yang berhubungan dengan subbab selanjutnya (polinom dan permutasi). Definisi dan macam-macam ring adalah sebagai berikut:

Definisi 2.4.1

Himpunan tidak kosong R dengan dua operasi biner, + dan $\cdot$ disimbolkan dengan $(R,+,\cdot)$ disebut *Ring* atau gelanggang jika memenuhi syarat-syarat berikut ini:

1. $(R,+)$ grup abel,
2. Operasi $\cdot$ tertutup pada R,
3. Pada Operasi $\cdot$ berlaku sifat asosiatif, dan
4. Memenuhi hukum distributif terhadap operasi pertama (Raisinghania dan Anggarwal, 1980:314).

Selanjutnya untuk mempermudah penulisan $(R,+,\cdot)$ akan ditulis R. Sedangkan $a \cdot b$ $(a,b \in R)$ ditulis ab.

Contoh 2.2

$(\mathbb{Z},+,\cdot)$ dengan $\mathbb{Z}$ himpunan bilangan bulat merupakan ring, karena:

1. $a,b \in \mathbb{Z} \rightarrow a+b \in \mathbb{Z}$ (Operasi + tertutup).

2. $a,b,c \in \mathbb{Z} \rightarrow (a+b)+c = a+b+c = a+(b+c)$ (Asosiatif penjumlahan).
3. $a,0 \in \mathbb{Z} \rightarrow a+0 = 0+a = a$ (0 Identitas operasi +).
4. $a,a^{-1} \in \mathbb{Z} \rightarrow a^{-1}+a = a+a^{-1} = 0 \Leftrightarrow a^{-1} = -a$ (Invers penjumlahan).
5. $a,b \in \mathbb{Z} \rightarrow a+b = b+a$ (Komutatif penjumlahan).
6. $a,b \in \mathbb{Z} \rightarrow ab \in \mathbb{Z}$ (Operasi $\times$ tertutup).
7. $a,b,c \in \mathbb{Z} \rightarrow (ab)c = abc = a(bc)$ (Asosiatif perkalian).
8. $a,1 \in \mathbb{Z} \rightarrow a1 = 1a = a$ (0 Identitas operasi $\cdot$).
9. $a,b,c \in \mathbb{Z} \rightarrow a(b+c) = (ab)+(ac)$

   $(a+b)c = (ac)+(bc)$.

Definisi 2.4.2

(i) Sebuah ring dikatakan Ring dengan satuan (**RS**) jika ring tersebut memiliki identitas terhadap operasi kedua.

(ii) Ring dikatakan komutatif (**RK**) jika operasi kedua bersifat komutatif.

(iii) *Integral Domain* (**ID**) adalah ring komutatif dengan satuan (**RKS**) di mana jika $a,b \in R$, $\cdot$ operasi kedua , dan $a \cdot b = 0$ maka $a = 0$ atau $b = 0$.

(iv) Ring disebut **Ring pembagian** (*Division Ring/Skew field*) jika tiap elemen (selain identitas operasi pertama) memiliki invers terhadap operasi kedua.

(v) *Division ring* yang komutatif terhadap operasi kedua adalah ***field*** (lapangan) (Lidl dan Niederreiter, 1997:11-12).

2.5 Polinom dan Permutasi

Definisi 2.5.1

Misalkan *R* ring, Polinom $f(x)$ dengan bentuk

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d + \ldots$$

di mana $a_i \in R$, x variabel tak tentu disebut juga **polinom atas ring R** (*Polynomial over R*). Pangkat terbesar dari *x* merupakan **derajat** dari $f(x)$ (Fraleigh, 2003:199).

Untuk mempermudah, maka bentuk $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d + \ldots$ memiliki $a_i = 0,\ \forall i > d$. Sehingga $f(x)$ menjadi

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d .$$

Definisi 2.5.2

Polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$ disebut **Polinom Integer** (Polinom atas $\mathbb{Z}$) jika $a_0, a_1, \ldots, a_d \in \mathbb{Z}$ (Hardy dan Wright, 2009:103).

Definisi 2.5.3

Permutasi adalah pemetaan satu-satu dari himpunan berhingga pada dirinya sendiri. Dengan kata lain, *A* himpunan berhingga, maka permutasi dari *A* adalah $g : A \to A$ dan *g* memetakan tiap elemen *A* tepat satu ke himpunan *A* itu sendiri (Raisinghania dan Anggarwal, 1980:115).

Definisi 2.5.4

Diberikan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$ dan modulo *p*, dengan *p* bilangan prima. Maka $f(x)$ disebut **Polinomial Permutasi (PP)** jika ada

fungsi f sedemikian hingga $f : x \to f(x)$ adalah permutasi pada modulo p. Dengan kata lain, $f(x)$ adalah PP dari modulo p jika dan hanya jika $f : x \to f(x)$ bersifat onto dan satu-satu (Shallue, 2012:6).

Contoh 2.3

Diberikan $g(x) = 3x^9 + 7x^8 + 4x^7 + 9x^6 + 8x^5 + 6x^4 + 2x^3 + 5x^2 + x + 1$ dan modulo 11 yaitu $\mathbb{Z}_{11} = \{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10]\}$.

Maka peta dari $\mathbb{Z}_{11}$ oleh $g(x)$ adalah

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$g(x)$	$[1]$	$[2]$	$[9]$	$[6]$	$[10]$	$[5]$	$[8]$	$[3]$	$[7]$	$[4]$	$[0]$

Dari hasil di atas diperoleh bahwa peta dari $\mathbb{Z}_{11}$ adalah $\mathbb{Z}_{11}$ itu sendiri. Jadi polinom $g(x)$ memperrmutasikan unsur $\mathbb{Z}_{11}$. Permutasinya adalah $([0]\ [1]\ [2]\ [9]\ [4]\ [10])\ ([3]\ [6]\ [8]\ [7])$.

Contoh 2.4

Diberikan $h(x) = x^2 + 3x + 5$. Maka peta dari $\mathbb{Z}_{11}$ oleh $h(x)$ adalah

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$h(x)$	$[5]$	$[9]$	$[4]$	$[1]$	$[0]$	$[1]$	$[4]$	$[9]$	$[5]$	$[3]$	$[3]$

Dari hasil di atas diperoleh bahwa ada beberapa unsur dari $\mathbb{Z}_{11}$ yang memiliki peta yang sama yaitu $x = [0]$ dengan $x = [8]$, $x = [1]$ dengan $x = [7]$, $x = [2]$ dengan $x = [6]m$, $x = [3]$ dengan $x = [5]$, dan $x = [9]$ dengan $x = [10]$. Jadi $h(x)$ bukan fungsi injektif, sehingga $h(x)$ tidak mempermutasikan unsur dari $\mathbb{Z}_{11}$.

Teorema 2.1

Jika $(d>1)|(p-1)$, $(d>1)$ membagi $(p-1)\left(\forall d, p \in \mathbb{Z}^{+}\right)$ maka tidak ada PP modulo p berderajat d (Lidl dan Niederreiter, 1997:349).

Bukti:

Diberikan $f(x)=a_0+a_1x+a_2x^2+\ldots+a_dx^d$ sehingga $\deg(f)=d$.

Sesuai teorema 7.4 (Lidl dan Niederreiter, 1997:349) yang menyebutkan bahwa jika $f(x)$ PP maka untuk setiap bilangan bulat t dengan $0\le t\le p-2$ berakibat $\deg\left(f(x)^t\right)\le p-2$.

Ambil $t=\frac{p-1}{d}$ maka $f(x)^{\frac{p-1}{d}}$ menjadi

$$\begin{aligned} f(x) &= \left(a_0+a_1x+a_2x^2+\ldots+a_dx^d\right)^{\frac{p-1}{d}} \\ &= a_0+a_1x+a_2x^2+\ldots+a_dx^{\frac{p-1}{d}d} \\ &= a_0+a_1x+a_2x^2+\ldots+a_dx^{p-1} \end{aligned}$$

berakibat $\deg\left(f^{\frac{p-1}{d}}\right)=p-1$.

Karena $\deg\left(f(x)^t\right)=p-1\not\le p-2$, jadi saat $\deg(f)=d$ dan $d|(p-1)$ maka tidak ada PP pada modulo *p*.

Teorema 2.2

Diberikan *GF(p)* dengan karakteristik berbeda dari 3. Maka $f(x)=ax^3+bx^2+cx+d\,(a\neq 0)$ mempermutasikan *GF(p)* jika dan hanya jika $b^2\equiv 3ac$ dan $p\equiv 2(\bmod 3)$ (Mollin dan Small, 1986:540).

GF(p) yang dimaksud adalah lapangan terbatas atau *Finite Field* dengan unsur sebanyak *p* dan *p* bilangan prima.

Bukti:

$(\Rightarrow)$

$f(x)$ mempermutasikan *GF(p)* jika dan hanya jika $x\left(x^2+ba^{-1}x+ca^{-1}\right)$ juga mempermutasikan *GF(p)*. Asumsikan $y=x+b(3a)^{-1}$ maka

$$x\left(x^2+ba^{-1}x+ca^{-1}\right)=y^3+c'y+d',$$

dengan $c'=\left(3ac-b^2\right)\left(3a^2\right)^{-1}$. Sehingga $f(x)$ mempermutasikan *GF(p)* jika dan hanya jika $x^3+\alpha x$ dengan $\alpha=\left(b^2-3ac\right)\left(3a^2\right)^{-1}$ juga mempermutasikan *GF(p)*. Sesuai teorema 2.8 (Mollin dan Small, 1986:540) yang menyebutkan bahwa jika $\alpha\neq 0$ dan $p\not\equiv 2(\mathrm{mod}\,3)$ maka $f(x)$ bukan PP pada *GF(p)*. Karena $f(x)$ PP *GF(p)* maka $\alpha=0$ berakibat $b^2=3ac$ dan $p\equiv 2(\mathrm{mod}\,3)$.

$(\Leftarrow)$

$f(x)$ mempermutasikan *GF(p)* jika dan hanya jika $x^3+\alpha x$ dengan $\alpha=\left(b^2-3ac\right)\left(3a^2\right)^{-1}$ juga mempermutasikan *GF(p)*. Karena $b^2=3ac$ dan $p\equiv 2(\mathrm{mod}\,3)$ maka $\alpha=0$ dan sesuai teorema 2.8 (Mollin dan Small, 1986:540) maka $f(x)$ mempermutasikan *GF(p)*. Lebih jelasnya diberikan contoh 2.5 sebagai berikut:

Contoh 2.5

Misalkan $m(x)=14+2x+4x^2+x^3=14+(2+4x+x^2)x$ dan *GF(p)* yang digunakan adalah $(\mathbb{Z}_5,+_5,\times_5)$. Pemetaan *GF(p)* oleh *m(x)* adalah sebagai berikut:

$m:[0]\to[4]$, $m:[1]\to[1]$, $m:[2]\to[2]$, $m:[3]\to[3]$, $m:[4]\to[0]$, dan permutasinya $([0][4])$.

Kemudian pemetaan *GF(p)* oleh $k(x)=(2+4x+x^2)x$ adalah:

$k:[0]\to[0]$, $k:[1]\to[2]$, $k:[2]\to[3]$, $k:[3]\to[4]$, $k:[4]\to[1]$, dan permutasinya $([1][2][3][4])$.

Jadi, sesuai teorema 2.2 *m(x)* PP pada *GF(p)* jika dan hanya jika *k(x)* PP pada *GF(p)*.

Selanjutnya, karena $m(x)=14+2x+4x^2+x^3$ maka $b^2\equiv 3ac$ atau

$$4^2\equiv 3\times 1\times 2(\mathrm{mod}\,5)$$

$$16\equiv 6(\mathrm{mod}\,5)$$

$$16\equiv 1(\mathrm{mod}\,5).$$

Dari contoh ini diperoleh bahwa *m(x)* mempermutasikan $\mathbb{Z}_5$ jika dan hanya jika $b^2\equiv 3ac$ dan $5\equiv 2(\mathrm{mod}\,3)$.

Teorema 2.3

Diberikan kongruensi

$$f(x)\equiv 0(\mathrm{mod}\,p^a) \qquad 2.1$$

dan

$$f(x) \equiv 0 \left(\mod p^{a-1}\right) \qquad 2.2$$

maka banyaknya solusi dari kongruensi 2.1 yang berkoresponden dengan satu solusi (yaitu ε) dari kongruensi 2.2 adalah satu jika

$f'(\varepsilon) \not\equiv 0 (\mod p)$ (Hardy dan Wright, 2009:124).

Bukti:

Andaikan c ($\forall c$ unsur dari domain fungsi f) akar dari kongruensi 2.1 yang mana $0 \le x < p^a$ maka $\forall n \ge 1$

$$\begin{aligned} f(x) &= (x-c) np^a \\ &= (x-c)(np)\, p^{a-1} \end{aligned}$$

Sehingga c juga memenuhi kongruensi 2.2.

Ambil $c = \varepsilon + sp^{a-1}$ dengan $(0 \le s < p)$. Jika ε adalah akar dari 2.2 dengan $\left(0 \le \varepsilon < p^{a-1}\right)$ maka sesuai deret taylor

$$f(c) = f\left(\varepsilon + sp^{a-1}\right) = f(\varepsilon) + sp^{a-1} f'(\varepsilon) + \frac{s^2 p^{2(a-1)}}{2} f''(\varepsilon) + \frac{s^3 p^{3(a-1)}}{6} f'''(\varepsilon) + \cdots$$

Karena $a > \frac{a}{n}$ maka $a - 1 \ge \frac{a}{n}$, $(n > 1, a > 1)$.

Saat $n = 2$ dan $a = 2$ maka $a - 1 = 2 - 1 = 1 = \frac{2}{2} = \frac{a}{n}$.

Saat $n > 2, a > 2$ dan $a < n$ maka $a - 1 > 1$ dan $\frac{a}{n} < 1$, sehingga $a - 1 > \frac{a}{n}$.

Saat $n > 2, a > 2$ dan $a > n$ maka

$$(a-1) - \frac{a}{n} = \frac{n(a-1) - a}{n} = \frac{(n-1)a - n}{n} > 0.$$

Karena $(a-1)-\frac{a}{n}>0$, maka $(a-1)>\frac{a}{n}$.

Jadi, $a-1\geq\frac{a}{n}$ atau $n(a-1)\geq a$, $(n>1, a>1)$.

Karena $n(a-1)\geq a, (n>1, a>1)$ maka $p^{n(a-1)}=p^{n(a-1)-a}p^a\equiv 0(\text{mod } p^a)$.

Lihat $\frac{f^{(k)}(\varepsilon)}{k!}$. Misalkan $f(x)=a_0+a_1x+a_2x^2+\ldots+a_dx^d$ maka

$$f'(\varepsilon)=a_1+2a_2\varepsilon+3a_2\varepsilon^2\ldots+da_d\varepsilon^{d-1}$$

$$f''(\varepsilon)=2a_2+(3\cdot 2)a_2\varepsilon^2\ldots+d(d-1)a_d\varepsilon^{d-2}$$

$$f'''(\varepsilon)=(3\cdot 2)a_2+(4\cdot 3\cdot 2)a_2\varepsilon+(5\cdot 4\cdot 3)a_2\varepsilon^2+\ldots+d(d-1)(d-2)a_d\varepsilon^{d-3}$$

Sehingga saat

$$\begin{aligned}f^{(k)}(\varepsilon)&=k(k-1)(k-2)k(k-3)\cdots(2\cdot 1)a_k+\ldots+d(d-1)(d-2)\cdots(d-k)a_d\varepsilon^{d-k-1}\\&=(k!)a_k+(k+1)(k!)a_k\varepsilon+\cdots+d(d-1)(d-2)\cdots(d-k)a_d\varepsilon^{d-k-1}\end{aligned}$$

Karena $k!$ membagi koefisien dari $f^{(k)}(\varepsilon)$, maka $\frac{f^{(k)}(\varepsilon)}{k!}$ merupakan bilangan bulat. Sehingga

$$\begin{aligned}s^k p^{k(a-1)}\frac{f^{(k)}(\varepsilon)}{k!}&=s^k\frac{f^{(k)}(\varepsilon)}{k!}p^{k(a-1)}\\&\equiv\left(s^k\frac{f^{(k)}(\varepsilon)}{k!}\right)\cdot 0(\text{mod } p^a)\\&\equiv 0(\text{mod } p^a)\end{aligned}$$

berakibat

$$f\left(\varepsilon + sp^{a-1}\right) \equiv f\left(\varepsilon\right) + sp^{a-1} f'\left(\varepsilon\right) + 0\left(\text{mod } p^a\right)$$
$$\equiv f\left(\varepsilon\right) + sp^{a-1} f'\left(\varepsilon\right)\left(\text{mod } p^a\right)$$

Kemudian, $\varepsilon + sp^{a-1}$ adalah akar dari kongruensi 2.1 jika dan hanya jika

$$f\left(\varepsilon + sp^{a-1}\right) \equiv 0\left(\text{mod } p^a\right)$$
$$f\left(\varepsilon\right) + sp^{a-1} f'\left(\varepsilon\right) \equiv 0\left(\text{mod } p^a\right)$$
$$\frac{f\left(\varepsilon\right) + sp^{a-1} f'\left(\varepsilon\right)}{p^{a-1}} \equiv \frac{0}{p^{a-1}}\left(\text{mod } p^a\right)$$
$$\frac{f\left(\varepsilon\right)}{p^{a-1}} + sf'\left(\varepsilon\right) \equiv 0\left(\text{mod } p^a\right)$$

Karena $f\left(\varepsilon\right) \equiv 0\left(\text{mod } p^{a-1}\right)$ atau $f\left(\varepsilon\right) \equiv np^{a-1}$, $\forall n \in \mathbb{Z}$ maka

$$\frac{f\left(\varepsilon\right)}{p^{a-1}} + sf'\left(\varepsilon\right) \equiv 0\left(\text{mod } p^a\right)$$
$$\frac{np^{a-1}}{p^{a-1}} + sf'\left(\varepsilon\right) \equiv 0\left(\text{mod } p^a\right)$$
$$n + sf'\left(\varepsilon\right) \equiv 0\left(\text{mod } p^a\right)$$

Karena $0\left(\text{mod } p^a\right)$ ekuivalen dengan $wp^a = \left(wp^{a-1}\right)p \equiv 0\left(\text{mod } p\right)$, $\forall w \in \mathbb{Z}$ maka

$$n + sf'\left(\varepsilon\right) \equiv 0\left(\text{mod } p\right)$$
$$sf'\left(\varepsilon\right) \equiv -n\left(\text{mod } p\right) \qquad 2.3$$

Karena $f'\left(\varepsilon\right) \not\equiv 0\left(\text{mod } p\right)$ maka membangkitkan setiap unsur dari modulo *p*. Sehingga hanya ada satu $s\left(\text{mod } p\right)$ yang memenuhi kongruensi 2.3.

Akibat 2.1

Misalkan p bilangan prima. $f(x)$ mempermutasikan elemen-elemen dari $\mathbb{Z}_{p^n}, n>1$ jika dan hanya jika $f(x)$ mempermutasikan elemen-elemen dari $\mathbb{Z}_p$ dan $f'(a) \not\equiv 0 \pmod{p}, \forall a \in \mathbb{Z}_p$ (Singh dan Maity, 2005:2).

Bukti:

$(\Rightarrow)$

Karena $f(x)$ mempermutasikan elemen-elemen dari $\mathbb{Z}_{p^n}$, $n>1$, maka $f(x)$ adalah fungsi satu-satu atau

$$f(x) \equiv 0 \pmod{p^n} \qquad 2.4$$

hanya memiliki satu akar, misalkan c. Sehingga

$$f(c) = (x-c)kp^n, \qquad \forall k \geq 1$$
$$= (x-c)\left(kp^{n-1}\right)p$$

maka c memenuhi

$$f(c) \equiv 0 \pmod{p} \qquad 2.5$$

Ambil $c = \varepsilon + sp^{a-1}$ dengan $(0 \leq s < p)$. Kemudian andaikan ε adalah akar dari 2.5 dengan $(0 \leq \varepsilon < p)$ dan $f'(a) \not\equiv 0 \pmod{p}, \forall a \in \mathbb{Z}_p$, maka sesuai teorema 2.3 $f(x) \equiv 0 \pmod{p^2}$ hanya memiliki satu akar yang berkoresponden dengan kongruensi 2.5. Sesuai teorema 2.3 juga, $f(x) \equiv 0 \pmod{p^3}$ hanya memiliki satu akar yang berkoresponden dengan $f(x) \equiv 0 \pmod{p^2}$, dan seterusnya. Sehingga

diperoleh $f(x) \equiv 0 \pmod{p^n}$ hanya memiliki satu akar yang berkorespondensi dengan solusi ε dari kongruensi 2.5 untuk setiap n >1.

$(\Leftarrow)$

Karena $f(x)$ mempermutasikan elemen-elemen dari $\mathbb{Z}_p$ maka $f(x)$ adalah fungsi satu-satu dan $f'(a) \not\equiv 0 \pmod{p}, \forall a \in \mathbb{Z}_p$. Sehingga sesuai teorema 2.3 $f(x)$ mempermutasikan elemen-elemen dari $\mathbb{Z}_{p^n}$.

2.6 Balasan Perbuatan Manusia dalam Pandangan Islam

Setiap masyarakat di dunia ini pasti memiliki sekumpulan peraturan berkenaan dengan kehidupan sosial mereka yang wajib dipatuhi oleh setiap individu dalam komunitasnya. Masing-masing anggota masyarakat tersebut berkewajiban menyesuaikan segala aktivitasnya sesuai dengan peraturan yang ada serta mengaitkannya satu sama lain sehingga lahir sebuah keserasian serta keharmonisan yang pada akhirnya mengantarkan mereka kepada pemenuhan segala kebutuhan dan tuntutan setiap anggota masyarakat, masing-masing berdasarkan kadar serta kualitas kebutuhan yang layak baginya (Thabathaba'i, 2005:157).

Ketika peraturan-peraturan dalam sebuah masyarakat ini berkaitan dengan kebebasan kehendak manusia (setiap individu bebas berkehendak untuk menaati atau melanggarnya) maka dalam menerapkan peraturan-peraturan tersebut diperlukan suatu langkah untuk sedikit membatasi kebebasan setiap individu dalam setiap sepak terjangnya. Sebab, manusia memiliki karakter yang selalu cenderung mengumbar kebebasannya dan tidak mau terikat oleh peraturan. Maka,

untuk menutupi kekurangan ini ditetapkanlah ketentuan penerapan sanksi bagi yang melanggar setiap peraturan, disamping ganjaran bagi yang melaksanakannya (Thabathaba'i, 2005:157).

Demikian pula dengan Syariat Islam yang telah Allah turunkan melalui para utusan-Nya. Dia Yang Maha Bijaksana menetapkan kebijakan yang sama. Allah berfirman dalam Surat Yunus ayat 26-27:

"*Bagi orang-orang yang berbuat (amal-amal) baik (dalam kehidupan dunia ini), ada pahala (ganjaran/balasan) yang terbaik (surga) dan (disertai) tambahannya. Dan muka mereka tidak ditutupi (sedikitpun oleh) debu hitam dan tidak (pula) kehinaan. Mereka itulah penghuni surga, mereka kekal di dalamnya. Dan orang-orang yang mengerjakan kejahatan (maka meraka mendapat) balasan yang setimpal (dengan dosa yang mereka lakukan, tanpa sedikit tambahan pun) dan mereka ditutupi kehinaan. Tidak ada bagi mereka seorang pelindungpun (yang dapat menghindarkan mereka) dari (azab) Allah, seakan-akan muka mereka ditutupi dengan kepingan-kepingan malam yang gelap gelita. Mereka itulah penghuni neraka; mereka kekal di dalamnya*" *(QS. Yunus:26-27).*

Pada ayat lain Allah berfirman:

"Dan balasan suatu kejahatan adalah kejahatan yang serupa (seimbang)(QS:Asy-Syura:40)".

Penetapan balasan dan sanksi memiliki kaitan erat dengan jenis serta kualitas pelaksanaan atau pelanggaran peraturan yang dilakukan. Artinya, perbuatan seseorang akan setimpal dengan jenis balasan atau sanksi yang ditimbulkannya. Semakin besar kadar kepatuhan seseorang terhadap peraturan, semakin besar pula balasan yang akan diterimanya. Demikian pula sebaliknya, semakin besar kualitas pelanggarannya maka semakin besar juga sanksi yang akan diterimanya (Thabathaba'i, 2005:158).

Allah telah menetapkan kunci kesuksesan dan kebahagiaan manusia adalah dengan menaati sekian banyak perintah, larangan, anjuran, kabar gembira,

dan peringatan. Allah menjanjikan balasan (yang baik) bagi yang melaksanakan perintah-Nya dan juga menyiapkan balasan (sanksi) bagi yang tidak menaati-Nya. Oleh karena itu, amal perbuatan seseorang di sisi Allah memiliki kaitan erat dengan balasan yang akan diterimanya, baik berupa kepatuhan terhadap semua perintah-Nya atau pelanggaran terhadap larangan-larangan-Nya (Thabathaba'i, 2005:159). Ini sesuai dengan ayat kelima belas dalam Surat Al-Jatsiyah yang berbunyi:

مَنْ عَمِلَ صَٰلِحًا فَلِنَفْسِهِۦ ۖ وَمَنْ أَسَآءَ فَعَلَيْهَا ۖ ثُمَّ إِلَىٰ رَبِّكُمْ تُرْجَعُونَ

Barang siapa yang mengerjakan amal saleh, maka itu adalah untuk dirinya sendiri, dan barang siapa yang mengerjakan kejahatan, maka itu akan menimpa dirinya sendiri, kemudian kepada Tuhanmulah kamu dikembalikan (QS. Al-Jatsiyah:15).

Al-Jazairi (2009:731-732) menjelaskan bahwa makna dari penggalan ayat "*Barang siapa yang mengerjakan amal saleh, maka itu adalah untuk dirinya sendiri*" adalah beramal shalih di dunia ini, yaitu beriman, taat kepada Allah dan rasul-Nya, baik dalam perintah maupun larangan, maka sesungguhnya Allah akan memasukkannya ke dalam surga. Dan amal shalihnya itu kembali kepada dirinya sendiri dan tidak berpindah kepada orang lain, sesungguhnya Allah tidak butuh kepada amalan hamba-hamba-Nya. Selanjutnya penggalan "*Barang siapa yang mengerjakan kejahatan, maka itu akan menimpa dirinya sendiri*" seperti tidak mengimani Allah, berbuat syirik, dan tidak beramal shalih, maka balasan atas perbuatan mereka itu akan kembali kepada dirinya, yaitu balasan berupa siksaan neraka dan kekal di dalamnya. Kemudian di bagian akhir ayat tersebut (*QS. Al-Jatsiyah:15*) menunjukkan bahwa setelah kematian masing-masing orang ada yang membawa amal shalih dan amal buruk, maka semua akan kembali kepada-

Nya dengan membawa amal masing-masing, sehingga pada hari kiamat Allah akan membalas setiap amal perbuatan yang dilakukan semasa hidup di dunia.

Selanjutnya Al-Jazairi menjelaskan bahwa dari ayat ini (*QS. Al-Jatsiyah:15*) mengandung dua poin penting. Pertama, sesungguhnya seseorang itu tidak akan disiksa karena kejahatan orang lain. Kedua, setiap amal perbuatan itu berpengaruh pada jiwa, sehingga menjadi sifat yang melekat padanya. Oleh karena itu, seseorang akan mendapatkan balasan di hari akhir dengan amalannya, baik berupa kebaikan maupun keburukan sesuai dengan apa yang telah dilakukan semasa hidupnya.

BAB III

PEMBAHASAN

3.1 Polinomial Permutasi Modulo p^n

Diberikan Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. Polinom $f(x)$ merupakan **Polinomial Permutasi** (**PP**) pada modulo $p^n\left(\mathbb{Z}_{p^n}\right)$ (p bilangan prima dan $n\in\mathbb{Z}^+$) jika pemetaan $f:c\to f(c)$, $\forall c\in\mathbb{Z}_{p^n}$ adalah permutasi dari $\mathbb{Z}_{p^n}$.

Contoh 3.1

Misalkan $h(x)=x^{10}+7x^8+4x^7+9x^6+6x^4+2x^3+5x^2+x$. Pemetaan modulo 16 $\left(2^4\right)$ oleh $h(x)$ sebagai berikut:

$h:[0]\to[0]$ $\quad$ $h:[8]\to[8]$

$h:[1]\to[3]$ $\quad$ $h:[9]\to[11]$

$h:[2]\to[6]$ $\quad$ $h:[10]\to[14]$

$h:[3]\to[9]$ $\quad$ $h:[11]\to[1]$

$h:[4]\to[4]$ $\quad$ $h:[12]\to[12]$

$h:[5]\to[7]$ $\quad$ $h:[13]\to[15]$

$h:[6]\to[10]$ $\quad$ $h:[14]\to[2]$

$h:[7]\to[13]$ $\quad$ $h:[15]\to[5]$

Sehingga permutasinya $([1][3][9][11])([2][6][10][14])([5][7][13][15])$.

3.2 Sifat Polinomial Permutasi Modulo 2^n

3.2.1 Polinomial Permutasi Modulo 2

Diberikan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. Misalkan pemetaan $f:x\to f(x)$ untuk setiap $x\in\mathbb{Z}_2$, maka untuk $x=[0](\mathrm{mod}\,2)$,

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$$

$$f([0])=a_0+a_1[0]+a_2[0]^2+\cdots+a_d[0]^d$$

$$=a_0+a_1[0]+a_2[0]+\cdots+a_d[0]$$

$$=a_0+(a_1+a_2+\cdots+a_d)[0]$$

dan untuk $x=[1](\mathrm{mod}\,2)$,

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$$

$$f([1])=a_0+a_1[1]+a_2[1]^2+\cdots+a_d[1]^d$$

$$=a_0+a_1[1]+a_2[1]+\cdots+a_d[1]$$

$$=a_0+(a_1+a_2+\cdots+a_d)[1]$$

Sehingga saat $x=[0]$ dan $x=[1]$ pada modulo 2 maka:

$$f(x)=a_0+(a_1+a_2+\cdots+a_d)x.$$

Andaikan $(a_1+a_2+\cdots+a_d)$ genap, maka $(a_1+a_2+\cdots+a_d)$ habis dibagi oleh 2 dengan kata lain $(a_1+a_2+\cdots+a_d)\equiv 0(\mathrm{mod}\,2)$ maka:

$$(a_1+a_2+\ldots+a_d)[0]=\underbrace{[0]+[0]+\cdots+[0]+[0]}_{\text{sebanyak }(a_1+a_2+\ldots+a_d)}=[0],$$

$$(a_1+a_2+\cdots+a_d)[1]=\underbrace{[1]+[1]+\cdots+[1]+[1]}_{\text{sebanyak } (a_1+a_2+\ldots+a_d)}$$

$$=\underbrace{([1]+[1])+([1]+[1])+\cdots+([1]+[1])}_{\text{sebanyak } \frac{(a_1+a_2+\ldots+a_d)}{2}}$$

$$=\underbrace{[0]+[0]+\cdots+[0]}_{\text{sebanyak } \frac{(a_1+a_2+\ldots+a_d)}{2}}$$

$$=[0]$$

Maka saat $x=[0]$,

$$f([0])=a_0+(a_1+a_2+\cdots+a_d)[0]$$

$$=a_0+[0]$$

dan untuk $x=[1]$,

$$f([1])=a_0+(a_1+a_2+\cdots+a_d)[1]$$

$$=a_0+[0]$$

Karena saat $x=[0]$dan $x=[1]$ mempunyai peta yang sama. Maka $f(x)$ bukan polinomial permutasi pada modulo 2. Jadi pengandaian salah sehingga $f(x)$ dapat mempermutasikan modulo 2 jika $(a_1+a_2+\cdots+a_d)\not\equiv 0(\mathrm{mod}\,2)$ atau $(a_1+a_2+\cdots+a_d)\equiv 1(\mathrm{mod}\,2)$. Ini berarti $(a_1+a_2+\cdots+a_d)$ dapat dibagi 2 sisa 1 atau $(a_1+a_2+\cdots+a_d)$ bilangan bulat ganjil $2n+1(\forall n\in\mathbb{Z})$. Dari hasil ini diperoleh sebuah teorema, yaitu:

Teorema 3.1

Diberikan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. $f(x)$ adalah PP modulo 2 jika dan hanya jika $(a_1+a_2+\cdots+a_d)$ bilangan ganjil (Singh dan Maity, 2005:3).

Bukti:

$(\Rightarrow)$

Misalkan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. Kemudian pemetaan $f:x\to f(x)$ untuk setiap $x\in\mathbb{Z}_2$, maka untuk $x=[0](\mathrm{mod}\,2)$,

$$\begin{aligned} f([0]) &= a_0+a_1[0]+a_2[0]^2+\cdots+a_d[0]^d \\ &= a_0+a_1[0]+a_2[0]+\cdots+a_d[0] \\ &= a_0+(a_1+a_2+\cdots+a_d)[0] \end{aligned}$$

dan untuk $x=[1](\mathrm{mod}\,2)$,

$$\begin{aligned} f([1]) &= a_0+a_1[1]+a_2[1]^2+\cdots+a_d[1]^d \\ &= a_0+a_1[1]+a_2[1]+\cdots+a_d[1] \\ &= a_0+(a_1+a_2+\cdots+a_d)[1] \end{aligned}$$

Sehingga saat $x=[0]$ dan $x=[1]$ pada modulo 2 maka:

$$f(x)=a_0+(a_1+a_2+\cdots+a_d)x.$$

Andaikan $(a_1+a_2+\cdots+a_d)$ genap, maka $(a_1+a_2+\cdots+a_d)$ habis dibagi oleh 2 atau $(a_1+a_2+\cdots+a_d)\equiv 0(\mathrm{mod}\,2)$ maka:

$$(a_1+a_2+\cdots+a_d)[0]=\underbrace{[0]+[0]+\cdots+[0]+[0]}_{\text{sebanyak } (a_1+a_2+\ldots+a_d)}=[0]$$

$$(a_1+a_2+\cdots+a_d)[1]=\underbrace{[1]+[1]+\cdots+[1]+[1]}_{\text{sebanyak } (a_1+a_2+\ldots+a_d)}$$

$$=\underbrace{([1]+[1])+([1]+[1])+\cdots+([1]+[1])}_{\text{sebanyak } \frac{(a_1+a_2+\ldots+a_d)}{2}}$$

$$=\underbrace{[0]+[0]+\cdots+[0]}_{\text{sebanyak } \frac{(a_1+a_2+\ldots+a_d)}{2}}$$

$$=[0]$$

Maka saat $x=[0]$,

$$f([0])=a_0+(a_1+a_2+\cdots+a_d)[0]$$

$$=a_0+[0]$$

dan untuk $x=[1]$,

$$f([1])=a_0+(a_1+a_2+\cdots+a_d)[1]$$

$$=a_0+[0]$$

Karena $x=[0]$ dan $x=[1]$ mempunyai peta yang sama. Maka $f(x)$ bukan polinomial permutasi pada modulo 2. Jadi pengandaian salah, sehingga $f(x)$ dapat mempermutasikan modulo 2 jika $(a_1+a_2+\cdots+a_d)\equiv 1(\mathrm{mod}\,2)$ atau

$(a_1+a_2+\cdots+a_d)$ dibagi 2 sisa 1 atau $(a_1+a_2+\cdots+a_d)$ bilangan bulat ganjil $2n+1(\forall n\in\mathbb{Z})$.

$(\Leftarrow)$

Misal $(a_1+a_2+\cdots+a_d)$ bilangan ganjil sehingga $(a_1+a_2+\cdots+a_d)\equiv 1(\mathrm{mod}\,2)$ maka:

$$(a_1+a_2+\cdots+a_d)[0]=\underbrace{[0]+[0]+\cdots+[0]+[0]}_{\text{sebanyak } (a_1+a_2+\ldots+a_d)}=[0]$$

$$(a_1+a_2+\cdots+a_d)[1]=\underbrace{[1]+[1]+\cdots+[1]+[1]}_{\text{sebanyak } (a_1+a_2+\ldots+a_d)-1}+[1]$$

$$=\underbrace{([1]+[1])+([1]+[1])+\cdots+([1]+[1])}_{\text{sebanyak } \frac{(a_1+a_2+\ldots+a_d)-1}{2}}+[1]$$

$$=\underbrace{[0]+[0]+\cdots+[0]}_{\text{sebanyak } \frac{(a_1+a_2+\ldots+a_d)}{2}}+[1]$$

$$=[0]+[1]$$

$$=[1]$$

1. Saat $x=[0]$,

$$f([0])=a_0+a_1[0]+a_2[0]^2+\cdots+a_d[0]^d$$

$$=a_0+a_1[0]+a_2[0]+\cdots+a_d[0]$$

$$=a_0+(a_1+a_2+\cdots+a_d)[0]$$

$$=a_0+[0]$$

2. Saat $x=[1]$,

$$f([1]) = a_0 + a_1[1] + a_2[1]^2 + \cdots + a_d[1]^d$$

$$= a_0 + a_1[1] + a_2[1] + \cdots + a_d[1]$$

$$= a_0 + (a_1 + a_2 + \cdots + a_d)[1]$$

$$= a_0 + [1]$$

Saat a_0 genap maka $a_0 \equiv 0 \pmod 2$ dan

$$f([0]) = a_0 + [0] = [0] + [0] = [0 + 0] = [0]$$

$$f([1]) = a_0 + [1] = [0] + [1] = [1 + 0] = [1]$$

Sehingga $f([0]) \to [0]$, $f([1]) \to [1]$ dan permutasi $f(x)$ adalah $([0])([1])$.

Saat a_0 ganjil maka $a_0 \equiv 1 \pmod 2$ dan

$$f([0]) = a_0 + [0] = [1] + [0] = [1 + 0] = [1]$$

$$f([1]) = a_0 + [1] = [1] + [1] = [1 + 1] = [2] = [0]$$

Sehingga $f([0]) \to [1]$, $f([1]) \to [0]$ dan permutasi adalah $([0][1])$.

Jadi terbukti bahwa saat $(a_1 + a_2 + \cdots + a_d)$ bilangan bulat ganjil maka $f(x)$ mempermutasikan modulo 2.

Contoh 3.2

Misal $g(x) = x^8 + 3x^6 - x^5 + 6x^4 + 2x^3 + 5x^2 + x$. Pemetaaan $\mathbb{Z}_2$ oleh $g(x)$ adalah:

$$g([0]) = [0]^8 + 3[0]^6 - [0]^5 + 6[0]^4 + 2[0]^3 + 5[0]^2 + [0] + 5$$

$$= [0] + 5$$

Karena $[5]=[1](\text{mod}\,2)$ maka $g([0])=[0]+[1]=[0+1]=[1]$.

$$g([1])=[1]^8+3[1]^6-[1]^5+6[1]^4+2[1]^3+5[1]^2+[1]+5$$

$$=(1+3-1+6+2+5+1)[1]+5$$

$$=21[1]+5$$

$$=[1]+5$$

Karena $[5]=[1](\text{mod}\,2)$ maka $g([1])=[1]+[1]=[1+1]=[2]=[0]$.

Jadi $g:[0]\to[1]$, $g:[1]\to[0]$ dan permutasinya $([0][1])$.

3.2.2 Polinomial Permutasi Modulo 2^n, $n>1$

Misalkan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. Menurut akibat 2.1 $f(x)$ PP modulo $2^n, n>1$ jika dan hanya jika $f(x)$ PP modulo 2 dan $f'(x)\not\equiv 0(\text{mod}\,2), \forall x\in\mathbb{Z}_2$.

Karena $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$, maka

$$f'(x)=a_1+2a_2x+3a_3x^2+4a_4x^3+\cdots+da_dx^{d-1} \qquad (3.1)$$

Saat $x=[0]$ maka

$$f'([0])=a_1+2a_2[0]+3a_3[0]^2+4a_4[0]^3+\cdots+da_d[0]^{d-1}$$

$$=a_1+2a_2[0]+3a_3[0]+4a_4[0]+\cdots+da_d[0]$$

$$=a_1+(2a_2+3a_3+4a_4+\cdots+da_d)[0]$$

$$=a_1+[0]$$

Saat $x=[1]$ maka

$$f'([1]) = a_1 + 2a_2[1] + 3a_3[1]^2 + 4a_4[1]^3 + \cdots + da_d[1]^{d-1}$$

$$= a_1 + 2a_2[1] + 3a_3[1] + 4a_4[1] + \cdots + da_d[1]$$

$$= a_1 + [0] + 3a_3[1] + [0] + 5a_5[1] + [0] + \cdots + da_d[1]$$

Saat d genap berarti $d \equiv 0 \pmod 2$, maka

$$f'([1]) = a_1 + [0] + 3a_3[1] + [0] + 5a_5[1] + [0] + \cdots + da_d[1]$$

$$= a_1 + 3a_3[1] + 5a_5[1] + \cdots + (d-1)a_{d-1}[1]$$

$$= a_1 + (a_3 + a_5 + \cdots + a_{d-1})[1]$$

Karena menurut akibat 2.1 $f'(x) \not\equiv 0 \pmod 2$, maka

$$f'([0]) \not\equiv 0 \pmod 2 \Rightarrow a_1 \not\equiv 0 \pmod 2$$

$$f'([1]) \not\equiv 0 \pmod 2 \text{ dan } d \equiv 0 \pmod 2 \Rightarrow a_1 + (a_3 + a_5 + \cdots + a_{d-1}) \not\equiv 0 \pmod 2$$

Sehingga diperoleh tiga ciri sebagai berikut:

1. $a_1 \not\equiv 0 \pmod 2$ atau $a_1 \not\equiv 1 \pmod 2$ a_1 bilangan bulat ganjil.
2. $a_1 + (a_3 + a_5 + \cdots + a_{d-1}) \not\equiv 0 \pmod 2$ atau $a_1 + (a_3 + a_5 + \cdots + a_{d-1})$ tidak genap. Karena a_1 bilangan bulat ganjil, maka $(a_3 + a_5 + \cdots + a_d)$ bilangan bulat genap.
3. Sesuai dengan teorema PP modulo 2 (teorema 3.1), $(a_1 + a_2 + \cdots + a_d)$ bilangan bulat ganjil, sedangkan menurut poin 1 dan 2 disebutkan bahwa a_1 ganjil, dan $(a_3 + a_5 + \cdots + a_{d-1})$ genap maka $(a_2 + a_4 + \cdots + a_d)$ genap.

Dari ketiga ciri tersebut, maka diperoleh teorema sebagai berikut:

Teorema 3.2

Diberikan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. Polinom $f(x)$ adalah **PP** modulo $2^n, n>1$ jika dan hanya jika:

1. a_1 bilangan bulat ganjil,
2. Saat d genap, $(a_2+a_4+a_6+\cdots+a_d)$ dan $(a_3+a_5+a_7+\cdots+a_{d-1})$ bilangan bulat genap (Singh dan Maity, 2005:3).

Bukti:

$(\Rightarrow)$

Karena $f(x)$ PP modulo $2^n, n>1$ maka sesuai akibat 2.1 $f(x)$ PP modulo 2 dan $f'(x)\not\equiv 0(\mathrm{mod}\,2), \forall x\in\mathbb{Z}_2$. Sehingga saat $x=[0](\mathrm{mod}\,2)$ maka

$$f'([0])=a_1+2a_2[0]+3a_3[0]^2+4a_4[0]^3+\cdots+da_d[0]^{d-1}$$
$$=a_1+[0]$$

Saat $x=[1](\mathrm{mod}\,2)$ dan d genap, maka

$$f'([1])=a_1+2a_2[1]+3a_3[1]^2+4a_4[1]^3+\cdots+(d-1)a_{d-1}[1]^{d-2}+[0]$$
$$=a_1+3a_3[1]+5a_5[1]+\cdots+(d-1)a_{d-1}[1]$$
$$=a_1+(a_3+a_5+\cdots+a_{d-1})[1]$$

Karena menurut akibat 2.1 $f'(x)\not\equiv 0(\mathrm{mod}\,2), \forall x\in\mathbb{Z}_2$, maka

$$f'([0])\not\equiv 0(\mathrm{mod}\,2)\Rightarrow a_1\not\equiv 0(\mathrm{mod}\,2)$$

$f'([1]) \not\equiv 0 (\mathrm{mod}\, 2)$ dan $d \equiv 0 (\mathrm{mod}\, 2) \Rightarrow a_1 + (a_3 + a_5 + \cdots + a_{d-1}) \not\equiv 0 (\mathrm{mod}\, 2)$

1. $f'([0]) \not\equiv 0 (\mathrm{mod}\, 2) \Rightarrow a_1 \not\equiv 0 (\mathrm{mod}\, 2)$ atau a_1 ganjil.
2. $f'([1]) \not\equiv 0 (\mathrm{mod}\, 2) \Rightarrow a_1 + (a_3 + a_5 + \cdots + a_{d-1}) \not\equiv 0 (\mathrm{mod}\, 2)$. Karena a_1 ganjil atau $[a_1] = [1] (\mathrm{mod}\, 2)$ maka

$$a_1 + (a_3 + a_5 + \cdots + a_{d-1}) = [1] \Rightarrow [1] + (a_3 + a_5 + \cdots + a_{d-1}) = [1]$$
$$\Rightarrow (a_3 + a_5 + \cdots + a_{d-1}) = [1] - [1]$$
$$\Rightarrow (a_3 + a_5 + \cdots + a_{d-1}) = [1-1]$$
$$\Rightarrow [(a_3 + a_5 + \cdots + a_{d-1})] = [0]$$

Sehingga diperoleh $(a_3 + a_5 + \cdots + a_{d-1}) \equiv 0 (\mathrm{mod}\, 2)$.

Sesuai teorema 3.1 karena $a_1 + (a_3 + a_5 + \cdots + a_{d-1}) \equiv 1 (\mathrm{mod}\, 2)$ maka $(a_2 + a_4 + \cdots + a_d) \equiv 1 (\mathrm{mod}\, 2)$. Dengan kata lain diperoleh bahwa a_1 bilangan bulat ganjil, $(a_2 + a_4 + \cdots + a_d)$ genap, dan $(a_3 + a_5 + \cdots + a_{d-1})$ genap.

$(\Leftarrow)$

Sesuai dengan teorema 3.1 maka $f(x)$ adalah PP modulo 2. Selanjutnya akan dibuktikan bahwa $f'(x) \not\equiv 0 (\mathrm{mod}\, 2), \forall x \in \mathbb{Z}_2$.

Karena saat $da_d x^{d-1} = [0] (\mathrm{mod}\, 2)$, $\forall x \in \mathbb{Z}_2$, maka

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + \cdots + da_d x^{d-1}$$
$$= a_1 + [0] + 3a_3 x^2 + [0] + 5a_5 x^4 + \cdots + da_d x^{d-1}$$
$$= a_1 + a_3 x^2 + a_5 x^4 \cdots + a_d x^{d-1}$$

Sehingga, saat $x=[0]$,

$$f'([0]) = a_1 + a_3[0]^2 + a_5[0]^4 + \cdots + a_d[0]^{d-1}$$

$$= a_1 + a_3[0] + a_5[0] + \cdots + a_d[0]$$

$$= a_1 + [0]$$

Karena a_1 bilangan bulat ganjil maka $f'([0]) \not\equiv 0 \pmod 2$.

Saat $x=[1]$,

$$f'([1]) = a_1 + a_3[1]^2 + a_5[1]^4 + \cdots + a_d[1]^{d-1}$$

$$= a_1 + a_3[1] + a_5[1] + \cdots + a_d[1]$$

$$= a_1 + (a_3 + a_5 + \cdots + a_d)[1]$$

Karena $a_1 + (a_3 + a_5 + \cdots + a_d)$ bilangan bulat ganjil, maka $f'([1]) \not\equiv 0 \pmod 2$.

Karena terbukti bahwa $f(x)$ PP modulo 2 dan $f'(x) \not\equiv 0 \pmod 2$, sesuai dengan akibat 2.1 maka $f(x)$ PP modulo 2^n.

Contoh 3.3

Misalkan $k(x) = 4x^7 - 3x^6 - x^4 + 2x^3 + 6x^2 + x - 13$. Pemetaan modulo 8 (2^3) oleh $k(x)$ sebagai berikut:

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$k(x)$	$[3]$	$[4]$	$[5]$	$[2]$	$[7]$	$[0]$	$[1]$	$[6]$

Sehingga permutasinya $([0][3][2][5])([1][4][7][6])$.

3.3 Sifat Polinomial Permutasi Modulo 3^n

3.3.1 Polinomial Permutasi Modulo 3

Misalkan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan koefisien-koefisiennya bilangan bulat $(a_0, a_1, \ldots, a_d \in \mathbb{Z})$ dan pemetaan $f : x \to f(x)$ untuk setiap $x \in \mathbb{Z}_3$, maka

$$f([0]) = a_0 + a_1[0] + a_2[0]^2 + a_3[0]^3 + a_4[0]^4 + a_5[0]^5 + a_6[0]^6 + \cdots + a_d[0]^d$$

$$= a_0 + a_1[0] + a_2[0] + a_3[0] + a_4[0] + a_5[0] + a_6[0] + \cdots + a_d[0]$$

$$= a_0 + [0]$$

$$f([1]) = a_0 + a_1[1] + a_2[1]^2 + a_3[0]^3 + a_4[1]^4 + a_5[1]^5 + a_6[1]^6 + \cdots + a_d[1]^d$$

$$= a_0 + a_1[1] + a_2[1] + a_3[1] + a_4[1] + a_5[1] + a_6[1] + \cdots + a_d[1]$$

$$= a_0 + a_1[1] + a_2[1]^2 + a_3[1] + a_4[1]^2 + a_5[1] + a_6[1]^2 + \cdots + a_d[1]^d$$

$$= a_0 + (a_1 + a_3 + a_5 + \cdots)[1] + (a_2 + a_4 + a_6 + \cdots)[1]^2$$

Batas $(a_1 + a_3 + a_5 + \cdots)$ dan $(a_2 + a_4 + a_6 + \cdots)$ adalah a_d atau kurang dari a_d.

$$f([2]) = a_0 + a_1[2] + a_2[2]^2 + a_3[2]^3 + a_4[2]^4 + a_5[2]^5 + a_6[2]^6 + \cdots + a_d[2]^d$$

Saat $i = 2m+1,\ \forall m \geq 1$ (ganjil) maka:

$$[2]^{2m+1} = \underbrace{[2]\times[2]\times\cdots\times[2]}_{\text{sebanyak } 2m}\times[2]$$

$$= \underbrace{([2]\times[2])\times([2]\times[2])\times\cdots\times([2]\times[2])}_{\text{sebanyak } m}\times[2]$$

$$= \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } m}\times[2]$$

$$= [2]$$

Saat $i = 2m,\ \forall m \geq 1$ (genap) maka:

$$[2]^{2m} = \underbrace{[2]\times[2]\times\cdots\times[2]}_{\text{sebanyak } 2m}$$

$$= \underbrace{([2]\times[2])\times([2]\times[2])\times\cdots\times([2]\times[2])}_{\text{sebanyak } m}$$

$$= \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } m}$$

$$= [1]$$

Karena $[2]^{2m} = [1] = [2]^2, \forall m \geq 1$ maka

$$f([2]) = a_0 + a_1[2] + a_2[2]^2 + a_3[2]^3 + a_4[2]^4 + a_5[2]^5 + a_6[2]^6 + \cdots + a_d[2]^d$$

$$= a_0 + a_1[2] + a_2[2]^2 + a_3[2] + a_4[2]^2 + a_5[2] + a_6[2]^2 + \cdots + a_d[2]^d$$

$$= a_0 + (a_1 + a_3 + a_5 + \cdots)[2] + (a_2 + a_4 + a_6 + \cdots)[2]^2$$

Batas $(a_1 + a_3 + a_5 + \cdots)$ dan $(a_2 + a_4 + a_6 + \cdots)$ adalah a_d atau kurang dari a_d.

Jadi untuk setiap $x \in \mathbb{Z}_3$, maka

$$f(x) = a_0 + (a_1 + a_3 + a_5 + \cdots)x + (a_2 + a_4 + a_6 + \cdots)x^2$$

Misalkan $A=(a_1+a_3+a_5+\cdots)$ dan $B=(a_2+a_4+a_6+\cdots)$ dengan batas A dan B adalah a_d atau kurang dari a_d, maka

$$f(x)=a_0+Ax+Bx^2.$$

Menurut teorema 2.1 disebutkan bahwa suatu polinom dengan derajat d tidak dapat membentuk permutasi pada modulo p jika $d \mid p-1$. Jadi karena $d=2$ dan $p-1=2$ dan $d \mid p-1$. Agar $f(x)$ merupakan PP modulo 3 maka $B\equiv 0 \pmod 3$. Kemudian $A\not\equiv 0 \pmod 3$ karena jika $A\equiv 0 \pmod 3$ maka $f(x)=a_0,\ \forall\, x\in\mathbb{Z}_3$. Sehingga diperoleh teorema sebagai berikut:

Teorema 3.3

Diberikan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$. $f(x)$ **PP** modulo 3 jika dan hanya jika saat d genap, $(a_1+a_3+a_5+\cdots)\not\equiv 0 \pmod 3$ dan $(a_2+a_4+a_6+\cdots)\equiv 0 \pmod 3$ (Singh dan Maity, 2005:3).

Keterangan: Batas $(a_1+a_3+a_5+\cdots)$ dan $(a_2+a_4+a_6+\cdots)$ adalah a_d atau kurang dari a_d. Misalkan, jika $a_d=a_{11}$ maka $(a_1+a_3+a_5+\cdots+a_{11})$ dan $(a_2+a_4+\cdots+a_{10})$.

Bukti:

$(\Rightarrow)$ Karena $f(x)=a_0+Ax+Bx^2$ untuk setiap $x\in\mathbb{Z}_3$ dan $f(x)$ PP modulo 3 dengan $A=(a_1+a_3+a_5+\cdots)$ dan $B=(a_2+a_4+a_6+\cdots)$, maka sesuai teorema 2.1, $B\equiv 0 \pmod 3$.

Kemudian jika $A \equiv 0 \pmod 3$, maka $f(x) = a_0 + [0]x + [0]x^2 = a_0 + [0]$ (untuk setiap $x \in \mathbb{Z}_3$). Ini berarti setiap $x \in \mathbb{Z}_3$ memiliki peta yang sama, sehingga $f(x)$ bukan PP modulo 3. Jadi, agar $f(x)$ PP modulo 3 maka $(a_1 + a_3 + a_5 + \cdots) \not\equiv 0 \pmod 3$ dan $(a_2 + a_4 + a_6 + \cdots) \equiv 0 \pmod 3$.

$(\Leftarrow)$

Karena $f(x) = a_0 + Ax + Bx^2$, dengan $A \not\equiv 0 \pmod 3$ dan $B \equiv 0 \pmod 3$ maka $f(x) = a_0 + Ax$. Sehingga diperoleh enam kondisi, yaitu :

1. Saat $a_0 = [0]$ dan $A = [1]$, maka $f(x) = [0] + [1]x$. Sehingga

   $f([0]) = [0] + [1][0] = [0]$,

   $f([1]) = [0] + [1][1] = [1]$, dan

   $f([2]) = [0] + [1][2] = [2]$.

   PP-nya adalah $([0])([1])([2])$.

2. Saat $a_0 = [0]$ dan $A = [2]$, maka $f(x) = [0] + [2]x$. Sehingga

   $f([0]) = [0] + [2][0] = [0]$,

   $f([1]) = [0] + [2][1] = [2]$, dan

   $f([0]) = [0] + [2][0] = [0]$.

   PP-nya adalah $([0])([1][2])$.

3. Saat $a_0 = [1]$ dan $A = [1]$, maka $f(x) = [1] + [1]x$. Sehingga

$f([0]) = [1] + [1][0] = [1]$,

$f([1]) = [1] + [1][1] = [2]$, dan

$f([2]) = [1] + [1][2] = [0]$.

PP-nya adalah $([0][1][2])$.

4. Saat $a_0 = [1]$ dan $A = [2]$, maka $f(x) = [1] + [2]x$. Sehingga

$f([0]) = [1] + [2][0] = [1]$,

$f([1]) = [1] + [2][1] = [0]$, dan

$f([2]) = [1] + [2][2] = [2]$.

PP-nya adalah $([0][1])([2])$.

5. Saat $a_0 = [2]$ dan $A = [1]$, maka $f(x) = [2] + [1]x$. Sehingga

$f([0]) = [2] + [1][0] = [2]$,

$f([1]) = [2] + [1][1] = [0]$, dan

$f([2]) = [2] + [1][2] = [1]$.

PP-nya adalah $([0][2][1])$.

6. Saat $a_0 = [2]$ dan $A = [2]$, maka $f(x) = [2] + [2]x$. Sehingga

$f([0]) = [2] + [2][0] = [2]$,

$f([1]) = [2] + [2][1] = [1]$, dan

$f([2]) = [2] + [2][2] = [0]$.

PP-nya adalah $([0][2])([1])$.

Keenam kondisi diatas menunjukkan bahwa $f(x)=a_0+Ax+Bx^2$ dengan $A\not\equiv 0 \pmod 3$ dan $B\equiv 0 \pmod 3$ maka $f(x)$ mempermutasikan $\mathbb{Z}_3$.

Contoh 3.4

Misalkan $l(x)=2x^7-6x^6-2x^5+2x^4-2x^3+x^2-10$. Pemetaan $\mathbb{Z}_3$ oleh $l(x)$ sebagai berikut:

$$l([0])=2[0]^7-6[0]^6-2[0]^5+2[0]^4-2[0]^3+[0]^2-10$$
$$=[0]-10$$
$$=[2]$$

$$l([1])=2[1]^7-6[1]^6-2[1]^5+2[1]^4-2[1]^3+[1]^2-10$$
$$=2[1]-6[1]-2[1]+2[1]-2[1]+[1]-10$$
$$=(2-6-2+2-2+1)[1]-10$$
$$=(-5-10)[1]$$
$$=-15[1]$$
$$=[0]$$

$$l([2]) = 2[2]^7 - 6[2]^6 - 2[2]^5 + 2[2]^4 - 2[2]^3 + [2]^2 - 10$$

$$= 2[2] - 6[1] - 2[2] + 2[1] - 2[2] + [1] - [1]$$

$$= (2-2-2)[2] + (-6+2+1-1)[1]$$

$$= (-2)[2] + (-4)[1]$$

$$= [2] + [2]$$

$$= [1]$$

Jadi $l:[0] \to [2]$, $l:[1] \to [0]$ dan $l:[2] \to [1]$. Sehingga permutasinya $([0][2][1])$.

3.3.2 Polinomial Permutasi Modulo $3^n (n > 1)$

Misalkan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan koefisien-koefisiennya bilangan bulat $a_0, a_1, \ldots, a_d \in \mathbb{Z}$. Menurut akibat 2.1 $f(x)$ PP modulo $3^n, n > 1$ jika dan hanya jika $f(x)$ PP modulo 3 dan $f'(x) \not\equiv 0 (\mathrm{mod}\, 3)$, untuk setiap x unsur di modulo 3.

Karena $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$, maka

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + \cdots + da_d x^{d-1}$$

$$= a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 5a_5 x^4 + 6a_6 x^5 + \cdots + da_d x^{d-1}$$

$$= a_1 + 2a_2 x + [0] + 4a_4 x^3 + 5a_5 x^4 + [0] + \cdots + da_d x^{d-1}$$

$$= a_1 + 2a_2 x + 4a_4 x^3 + 5a_5 x^4 + \cdots + da_d x^{d-1}$$

Saat $x = [0] (\mathrm{mod}\, 3)$ maka

$$f'([0]) = a_1 + 2a_2[0] + 4a_4[0]^3 + 5a_5[0]^4 + \cdots + da_d[0]^{d-1}$$

$$= a_1 + [0]$$

Saat $x = [1] (\mathrm{mod}\, 3)$ maka

$$f'([1]) = a_1 + 2a_2[1] + 4a_4[1]^3 + 5a_5[1]^2 + \cdots + da_d[1]^{d-1}$$

$$= a_1 + 2a_2[1] + 4a_4[1] + 5a_5[1] + \cdots + da_d[1]^{d-1}$$

$$= a_1 + (2a_2 + 4a_4 + 5a_5 + \cdots + da_d)[1]$$

Karena pada modulo 3 berlaku $1, 4, 7, 10, 13,$ dan seterusnya kongruen dengan $1 (\mathrm{mod}\, 3)$. Sedangkan $2, 5, 8, 11, 14,$ dan seterusnya kongruen dengan $2 (\mathrm{mod}\, 3)$, maka

$$f'([1]) = a_1 + (2a_2 + 4a_4 + 5a_5 + 7a_7 + 8a_8 + 10a_{10} + 11a_{11} + \cdots + da_d)[1]$$

$$= a_1 + (2a_2 + a_4 + 2a_5 + a_7 + 2a_8 + a_{10} + 2a_{11} + \cdots + da_d)[1]$$

$$= (a_1 + 2a_2 + a_4 + 2a_5 + a_7 + 2a_8 + a_{10} + 2a_{11} + \cdots + da_d)[1]$$

$$= T[1] + U[1]$$

dengan:

$T = (a_1 + a_4 + a_7 + a_{10} + \cdots)$, dan

$U = (2a_2 + 2a_5 + 2a_8 + 2a_{11} + \cdots)$

$= 2(a_2 + a_5 + a_8 + a_{11} + \cdots)$

Keterangan: T dan U adalah deret dengan batas da_d atau kurang dari da_d. Misalnya, jika $da_d = a_{11}$ maka batas T adalah a_{10} dan batas U adalah a_{11}.

Saat $x=[2](\mathrm{mod}\,3)$ maka

$$f'([2]) = a_1 + 2a_2[2] + 4a_4[2]^3 + 5a_5[2]^4 + 7a_7[2]^6 + 8a_8[2]^7 + \cdots + da_d[2]^{d-1}$$

$$= a_1 + 2a_2[2] + 4a_4[2] + 5a_5[1] + 7a_7[1] + 8a_8[2] + \cdots + da_d[2]^{d-1}$$

Karena pada modulo 3 berlaku $1,4,7,10,13,$ dan seterusnya kongruen dengan $1(\mathrm{mod}\,3)$. Sedangkan $2,5,8,11,14,$ dan seterusnya kongruen dengan $2(\mathrm{mod}\,3)$, maka

$$f'([2]) = a_1 + 2a_2[2] + a_4[2] + 2a_5[1] + a_7[1] + 2a_8[2] + a_{10}[2] + 2a_{11}[1] + \cdots + da_d[2]^{d-1}$$

$$= a_1[1] + a_2[1] + a_4[2] + a_5[2] + a_7[1] + a_8[1] + a_{10}[2] + a_{11}[2] + \cdots + da_d[2]^{d-1}$$

$$= M[1] + N[2]$$

dengan:

$M = (a_1 + a_2 + a_7 + a_8 + \cdots)$, dan

$N = (a_4 + a_5 + a_{10} + a_{11} + \cdots)$.

Keterangan: M dan N adalah deret dengan batas da_d atau kurang dari da_d. Misalnya, jika $da_d = a_{11}$ maka batas M adalah a_8 dan batas N adalah a_{11}.

Karena menurut akibat 2.1 $f'(x) \not\equiv 0(\mathrm{mod}\,3)$, maka

$f'([0]) \not\equiv 0(\mathrm{mod}\,3) \Rightarrow a_1 \not\equiv 0(\mathrm{mod}\,3)$,

$f'([1]) \not\equiv 0(\mathrm{mod}\,3) \Rightarrow T[1] + U[2] \not\equiv 0(\mathrm{mod}\,3)$, dan

$f'([2]) \not\equiv 0(\mathrm{mod}\,3) \Rightarrow M[1] + N[2] \not\equiv 0(\mathrm{mod}\,3)$.

Sehingga sesuai teorema 2.1, $f(x)$ PP modulo 3 dan $f'(x) \not\equiv 0 \pmod 3$ diperoleh lima ciri, yaitu:

1. $a_1 \not\equiv 0 \pmod 3$,
2. $(a_1 + a_3 + a_5 + \cdots) \not\equiv 0 \pmod 3$,
3. $(a_2 + a_4 + a_6 + \cdots) \equiv 0 \pmod 3$,
4. $T[1] + U[2] \not\equiv 0 \pmod 3$, dan
5. $M[1] + N[2] \not\equiv 0 \pmod 3$.

Keterangan:

$T = (a_1 + a_4 + a_7 + a_{10} + \cdots)$,

$U = 2(a_2 + a_5 + a_8 + a_{11} + \cdots)$,

$M = (a_1 + a_2 + a_7 + a_8 + \cdots)$, dan

$N = (a_4 + a_5 + a_{10} + a_{11} + \cdots)$.

Keterangan: Poin 2 sampai 5 merupakan deret dengan batas da_d atau kurang dari da_d. Misalnya, jika $da_d = a_{11}$ maka batas poin 2 adalah a_{11}, batas poin 3 adalah a_{10}, batas T adalah a_{10}, batas U adalah a_{11}, batas M adalah a_8, dan batas N adalah a_{11}.

Dari ciri-ciri tersebut, maka diperoleh teorema sebagai berikut:

Teorema 3.4

Diberikan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan $a_0, a_1, \ldots, a_d \in \mathbb{Z}$. Maka $f(x)$ adalah **PP** modulo $3^n, n > 1$ jika dan hanya jika

a. $a_1 \not\equiv 0 \pmod 3$,

b. $(a_1 + a_3 + a_5 + \cdots) \not\equiv 0 \pmod 3$,

c. $(a_2 + a_4 + a_6 + \cdots) \equiv 0 \pmod 3$,

d. $T[1] + U[2] \not\equiv 0 \pmod 3$, dan

e. $M[1] + N[2] \not\equiv 0 \pmod 3$.

dengan:

$T = (a_1 + a_4 + a_7 + a_{10} + \cdots)$,

$U = 2(a_2 + a_5 + a_8 + a_{11} + \cdots)$,

$M = (a_1 + a_2 + a_7 + a_8 + \cdots)$, dan

$N = (a_4 + a_5 + a_{10} + a_{11} + \cdots)$.

Keterangan: Poin b sampai e merupakan deret dengan batas da_d atau kurang dari da_d. Misalnya, jika $da_d = a_{11}$ maka batas poin b adalah a_{11}, batas poin c adalah a_{10}, batas T adalah a_{10}, batas U adalah a_{11}, batas M adalah a_8, dan batas N adalah a_{11}.

Bukti:

$(\Rightarrow)$

Misalkan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan koefisien-koefisiennya bilangan bulat $(a_0, a_1, \ldots, a_d \in \mathbb{Z})$. Menurut akibat 2.1 $f(x)$ PP modulo $3^n, n > 1$ jika dan hanya jika $f(x)$ PP modulo 3 dan $f'(x) \not\equiv 0 \pmod 3$, untuk setiap x unsur di modulo 3.

Jadi saat $x = [0]$, maka $f'([0]) = a_1 + [0]$.

Saat $x = [0] \pmod 3$, maka

$$f'([0]) = a_1 + 2a_2[0] + 4a_4[0]^3 + 5a_5[0]^4 + \cdots + da_d[0]^{d-1}$$
$$= a_1 + [0]$$

Saat $x = [1] \pmod 3$, maka

$$f'([1]) = a_1 + 2a_2[1] + 4a_4[1]^3 + 5a_5[1]^5 + 7a_7[1]^6 + 8a_8[1]^7 + \cdots + da_d[1]^{d-1}$$
$$= a_1 + 2a_2[1] + 4a_4[1] + 5a_5[1] + 7a_7[1] + 8a_8[1] + \cdots + da_d[1]^{d-1}$$
$$= a_1 + (2a_2 + 4a_4 + 5a_5 + 7a_7 + 8a_8 + \cdots + da_d)[1]$$

Karena pada modulo 3 berlaku $1, 4, 7, 10, 13,$ dan seterusnya kongruen dengan $1 \pmod 3$. Sedangkan $2, 5, 8, 11, 14,$ dan seterusnya kongruen dengan $2 \pmod 3$, maka

$$f'([1]) = a_1 + (2a_2 + 4a_4 + 5a_5 + 7a_7 + 8a_8 + 10a_{10} + 11a_{11} + \cdots + da_d)[1]$$

$$= a_1 + (2a_2 + a_4 + 2a_5 + a_7 + 2a_8 + a_{10} + 2a_{11} + \cdots + da_d)[1]$$

$$= (a_1 + 2a_2 + a_4 + 2a_5 + a_7 + 2a_8 + a_{10} + 2a_{11} + \cdots + da_d)[1]$$

$$= T[1] + U[1]$$

dengan:

$T = (a_1 + a_4 + a_7 + a_{10} + \cdots)[1]$, dan

$U = (2a_2 + 2a_5 + 2a_8 + 2a_{11} + \cdots)[1]$

$= 2(a_2 + a_5 + a_8 + a_{11} + \cdots)[1]$

Saat $x = [2] (\mathrm{mod}\, 3)$ maka

$$f'([2]) = a_1 + 2a_2[2] + 4a_4[2]^3 + 5a_5[2]^4 + 7a_7[2]^6 + 8a_8[2]^7 + \cdots + da_d[2]^{d-1}$$

$$= a_1 + 2a_2[2] + 4a_4[2] + 5a_5[1] + 7a_7[1] + 8a_8[2] + \cdots + da_d[2]^{d-1}$$

Karena pada modulo 3 berlaku $1, 4, 7, 10, 13,$ dan seterusnya kongruen dengan $1 (\mathrm{mod}\, 3)$. Sedangkan $2, 5, 8, 11, 14,$ dan seterusnya kongruen dengan $2 (\mathrm{mod}\, 3)$, maka

$$f'([2]) = a_1 + 2a_2[2] + a_4[2] + 2a_5[1] + a_7[1] + 2a_8[2] + a_{10}[2] + 2a_{11}[1] + \cdots + da_d[2]^{d-1}$$

$$= a_1[1] + a_2[1] + a_4[2] + a_5[2] + a_7[1] + a_8[1] + a_{10}[2] + a_{11}[2] + \cdots + da_d[2]^{d-1}$$

$$= M[1] + N[2]$$

dengan $M = (a_1 + a_2 + a_7 + a_8 + \cdots)$ dan $N = (a_4 + a_5 + a_{10} + a_{11} + \cdots)$.

Karena menurut akibat 2.1 $f'(x) \not\equiv 0 (\mathrm{mod}\, 3)$, maka

$f'([0]) \not\equiv 0 \pmod 3 \Rightarrow a_1 \not\equiv 0 \pmod 3$,

$f'([1]) \not\equiv 0 \pmod 3 \Rightarrow T[1]+U[2] \not\equiv 0 \pmod 3$, dan

$f'([2]) \not\equiv 0 \pmod 3 \Rightarrow M[1]+N[2] \not\equiv 0 \pmod 3$.

Sehingga sesuai akibat 2.1, $f(x)$ PP modulo 3 dan $f'(x) \not\equiv 0 \pmod 3$ diperoleh lima ciri sesuai teorema 3.4.

$(\Leftarrow)$

Diberikan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d$ dengan $a_0, a_1, \ldots, a_d \in \mathbb{Z}$ dan ciri-ciri sebagai berikut:

a. $a_1 \not\equiv 0 \pmod 3$,

b. $(a_1 + a_3 + a_5 + \cdots) \not\equiv 0 \pmod 3$,

c. $(a_2 + a_4 + a_6 + \cdots) \equiv 0 \pmod 3$,

d. $T[1]+U[2] \not\equiv 0 \pmod 3$, dan

e. $M[1]+N[2] \not\equiv 0 \pmod 3$.

Sesuai akibat 2.1 yang menunjukkan bahwa polinom $f(x)$ merupakan PP modulo 3^n jika dan hanya jika $f(x)$ PP modulo 3 dan $f'(x) \not\equiv 0 \pmod 3$, $\forall x \in \mathbb{Z}_3$. Poin b dan c diatas sesuai dengan teorema sebelumnya (teorema 3.3) maka $f(x)$ PP modulo 3. Kemudian akan ditunjukkan bahwa $f'(x) \not\equiv 0 \pmod 3$, $\forall x \in \mathbb{Z}_3$.

Karena menurut akibat 2.1 $f'(x) \not\equiv 0 \pmod 3$, maka

$f'([0]) \not\equiv 0 \pmod 3 \Rightarrow a_1 \not\equiv 0 \pmod 3$,

$f'([1]) \not\equiv 0 \pmod 3 \Rightarrow T[1]+U[2] \not\equiv 0 \pmod 3$, dan

$f'([2]) \not\equiv 0 \pmod 3 \Rightarrow M[1]+N[2] \not\equiv 0 \pmod 3$.

Jadi terbukti bahwa $f(x)$ PP modulo 3 dan $f'(x) \not\equiv 0 \pmod 3$, $\forall x \in \mathbb{Z}_3$.

Contoh 3.5

Diberikan $p(x) = 4x^7 - 5x - 3$ dan $\mathbb{Z}_9$. Maka $p : \mathbb{Z}_9 \to \mathbb{Z}_9$ sebagai berikut:

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$
$p(x)$	$[6]$	$[5]$	$[4]$	$[0]$	$[2]$	$[1]$	$[3]$	$[8]$	$[7]$

Sehingga permutasinya $([0][6][3])([1][5])([2][4])([7][8])$.

3.4 Sifat Polinomial Permutasi Modulo 5^n

3.4.1 Polinomial Permutasi Modulo 5

Misalkan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan koefisien-koefisiennya bilangan bulat $(a_0, a_1, \ldots, a_d \in \mathbb{Z})$ dan pemetaan $f : x \to f(x)$ untuk setiap $x \in \mathbb{Z}_5$, maka

Saat $i = 4m+1$, $\forall m \geq 0$,

$$[0]^{4m+1} = \underbrace{[0] \times [0] \times \cdots \times [0]}_{\text{sebanyak } 4m} \times [0] = [0]$$

$$[1]^{4m+1} = \underbrace{[1] \times [1] \times \cdots \times [1]}_{\text{sebanyak } 4m} \times [1] = [1]$$

$$[2]^{4m+1} = \underbrace{[2]\times[2]\times\cdots\times[2]}_{\text{sebanyak } 4m}\times[2]$$

$$= \underbrace{([2]\times[2])\times([2]\times[2])\times\cdots\times([2]\times[2])}_{\text{sebanyak } 2m}\times[2]$$

$$= \underbrace{([4]\times[4])\times([4]\times[4])\times\cdots\times([4]\times[4])}_{\text{sebanyak } m}\times[2]$$

$$= \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } m}\times[2]$$

$$= [2]$$

$$[3]^{4m+1} = \underbrace{[3]\times[3]\times\cdots\times[3]}_{\text{sebanyak } 4m}\times[3]$$

$$= \underbrace{([3]\times[3])\times([3]\times[3])\times\cdots\times([3]\times[3])}_{\text{sebanyak } 2m}\times[3]$$

$$= \underbrace{([9]\times[9])\times([9]\times[9])\times\cdots\times([9]\times[9])}_{\text{sebanyak } m}\times[3]$$

$$= \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } m}\times[3]$$

$$= [3]$$

$$[4]^{4m+1} = \underbrace{[4]\times[4]\times\cdots\times[4]}_{\text{sebanyak } 4m}\times[4]$$

$$= \underbrace{([4]\times[4])\times([4]\times[4])\times\cdots\times([4]\times[4])}_{\text{sebanyak } 2m}\times[4]$$

$$= \underbrace{([1]\times[1])\times([1]\times[1])\times\cdots\times([1]\times[1])}_{\text{sebanyak } m}\times[4]$$

$$= [4]$$

Saat $i = 4m+2,\ \forall m \geq 0$,

$$[0]^{4m+2} = \underbrace{[0]\times[0]\times\cdots\times[0]}_{\text{sebanyak } 4m}\times[0]^2 = [0]^2$$

$$[1]^{4m+2} = \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } 4m}\times[1]^2 = [1]^2$$

$$[2]^{4m+2} = \underbrace{[2]\times[2]\times\cdots\times[2]}_{\text{sebanyak } 4m}\times[2]^2 = [2]^2$$

$$[3]^{4m+2} = \underbrace{[3]\times[3]\times\cdots\times[3]}_{\text{sebanyak } 4m}\times[3]^2 = [3]^2$$

$$[4]^{4m+2} = \underbrace{[4]\times[4]\times\cdots\times[4]}_{\text{sebanyak } 4m}\times[4]^2 = [4]^2$$

Saat $i = 4m+3,\ \forall m \geq 0$,

$$[0]^{4m+3} = \underbrace{[0]\times[0]\times\cdots\times[0]}_{\text{sebanyak } 4m}\times[0]^3 = [0]^3$$

$$[1]^{4m+3} = \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } 4m}\times[1]^3 = [1]^3$$

$$[2]^{4m+3} = \underbrace{[2]\times[2]\times\cdots\times[2]}_{\text{sebanyak } 4m}\times[2]^3 = [2]^3$$

$$[3]^{4m+3} = \underbrace{[3]\times[3]\times\cdots\times[3]}_{\text{sebanyak } 4m}\times[3]^3 = [3]^3$$

$$[4]^{4m+3} = \underbrace{[4]\times[4]\times\cdots\times[4]}_{\text{sebanyak } 4m}\times[4]^3 = [4]^3$$

Saat $i = 4m,\ \forall m \geq 0$,

$$[0]^{4m} = \underbrace{[0]\times[0]\times\cdots\times[0]}_{\text{sebanyak } 4m-4}\times[0]^4 = [0]^4$$

$$[1]^{4m} = \underbrace{[1]\times[1]\times\cdots\times[1]}_{\text{sebanyak } 4m-4}\times[1]^4 = [1]^4$$

$$[2]^{4m} = \underbrace{[2]\times[2]\times\cdots\times[2]}_{\text{sebanyak } 4m-4}\times[2]^4 = [2]^4$$

$$[3]^{4m} = \underbrace{[3]\times[3]\times\cdots\times[3]}_{\text{sebanyak } 4m-4}\times[3]^4 = [3]^4$$

$$[4]^{4m} = \underbrace{[4]\times[4]\times\cdots\times[4]}_{\text{sebanyak } 4m-4}\times[4]^4 = [4]^4$$

Sehingga diperoleh $[x]^{4m+1} = [x]$, $[x]^{4m+2} = [x]^2$, $[x]^{4m+3} = [x]^3$ dan $[x]^{4m} = [x]^4$ $\forall [x] \in M_5, m \geq 0$. Maka

$$f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4$$

dengan $A = (a_1 + a_5 + \cdots + a_{d-3})$, $B = (a_2 + a_6 + \cdots + a_{d-2})$, $C = (a_3 + a_7 + \cdots + a_{d-1})$, dan $D = (a_4 + a_8 + \cdots + a_d)$, $\forall d = 4m$, $m \geq 1$.

Menurut teorema 2.1 disebutkan bahwa suatu polinom dengan derajat d tidak dapat membentuk permutasi pada modulo p jika $d \mid (p-1)$. Karena $f(x)$ berderajat $d = 4$ dan $p - 1 = 4$ dan $d \mid (p-1)$, maka agar $f(x)$ PP pada $\mathbb{Z}_5$ $D \equiv 0 \pmod 5$. Sehingga

$$f(x) = a_0 + Ax + Bx^2 + Cx^3$$

Kemudian sesuai teorema 2.2 $f(x)$ merupakan PP $\mathbb{Z}_5$ jika dan hanya jika $B^2 \equiv 3AC$. Jadi diperoleh teorema sebagai berikut:

Teorema 3.5

Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$ maka $f(x)$ **PP** pada $\mathbb{Z}_5$, jika dan hanya jika $\forall d=4m,\ m\geq 1$, memenuhi:

1. $(a_2+a_6+\cdots+a_{d-2})^2\equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$
2. $(a_4+a_8+\cdots+a_d)\equiv 0(\mathrm{mod}\,5)$ (Singh dan Maity, 2005:5).

Bukti:

$(\Rightarrow)$

Sesuai $\mathbb{Z}_5$ bentuk $f(x)$ menjadi

$$f(x)=a_0+Ax+Bx^2+Cx^3+Dx^4$$

dengan $A=(a_1+a_5+\cdots+a_{d-3})$, $B=(a_2+a_6+\cdots+a_{d-2})$, $C=(a_3+a_7+\cdots+a_{d-1})$ dan $D=(a_4+a_8+\cdots+a_d)$, $\forall d=4m,\ m\geq 1$.

Menurut teorema 2.1 $f(x)$ merupakan PP pada $\mathbb{Z}_5$ jika $D\equiv 0(\mathrm{mod}\,5)$. Sehingga

$$f(x)=a_0+Ax+Bx^2+Cx^3.$$

Lalu sesuai teorema 2.2 $f(x)$ adalah PP pada $\mathbb{Z}_5$ jika dan hanya jika $B^2\equiv 3AC$.

$(\Leftarrow)$

Sesuai $\mathbb{Z}_5$ bentuk $f(x)$ menjadi

$$f(x)=a_0+Ax+Bx^2+Cx^3+Dx^4$$

dengan $A=(a_1+a_5+\cdots+a_{d-3})$, $B=(a_2+a_6+\cdots+a_{d-2})$, $C=(a_3+a_7+\cdots+a_{d-1})$ dan $D=(a_4+a_8+\cdots+a_d)$, $\forall d=4m,\ m\geq 1$. Diketahui bahwa $B^2\equiv 3AC$ dan $D\equiv 0(\mathrm{mod}\,5)$. Sehingga $f(x)$ menjadi

$$f(x)=a_0+Ax+Bx^2+Cx^3$$

Maka sesuai teorema 2.1 dan teorema 2.2 $f(x)$ adalah PP modulo 5.

Contoh 3.6

Misalkan $m(x)=14+2x+4x^2+x^3$. Jika $x\in\mathbb{Z}_5$ maka pemetaan $m(x)$ terhadap $\mathbb{Z}_5$ sebagai berikut:

$m([0])=14+2[0]+4[0]^2+[0]^3=14+[0]$

karena $14\equiv 4(\mathrm{mod}\,5)$ maka

$m([0])=[4]+[0]=[4]$

$m([1])=14+2[1]+4[1]^2+[1]^3$

$=14+[2]+[4]+[1]$

$=14+[2]$

$=[4]+[2]=[1]$

$m([2])=14+2[2]+4[2]^2+[2]^3$

$=14+[4]+[1]+[3]$

$=[2]$

$$m([3]) = 14 + 2[3] + 4[3]^2 + [3]^3$$

$$= 14 + [1] + [1] + [2]$$

$$= [3]$$

$$m([4]) = 14 + 2[4] + 4[4]^2 + [4]^3$$

$$= 14 + [3] + [4] + [4]$$

$$= [0]$$

Jadi $m:[0] \to [4]$, $m:[1] \to [1], m:[2] \to [2]$, $m:[3] \to [3]$ dan $m:[4] \to [0]$. Sehingga permutasinya $([0][4])$.

3.4.2 Polinomial Permutasi Modulo 5^n

Misalkan polinom $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan koefisien-koefisiennya bilangan bulat $(a_0, a_1, \ldots, a_d \in \mathbb{Z})$. Menurut akibat 2.1 $f(x)$ PP modulo $5^n, n > 1$ jika dan hanya jika $f(x)$ PP modulo 5 dan $f'(x) \not\equiv 0 \pmod 5$, untuk setiap x unsur di modulo 5.

Karena $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$, maka

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + \cdots + da_d x^{d-1}$$

$$= a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 5a_5 x^4 + 6a_6 x^5 + \cdots + da_d x^{d-1}$$

$$= a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + [0] + 6a_6 x^5 + \cdots + da_d x^{d-1}$$

$$= a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 6a_6 x^5 + \cdots + da_d x^{d-1} + [0]$$

$$= a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 6a_6 x^5 + \cdots + da_d x^{d-1}$$

Saat $x=[0](\mathrm{mod}\,5)$ maka

$$f'([0])=a_1+2a_2[0]+3a_3[0]^2+4a_4[0]^3+6a_6[0]^5+\cdots+da_d[0]^{d-1}$$

$$=a_1+[0]$$

Saat $x=[1](\mathrm{mod}\,5)$ maka

$$f'([1])=a_1+2a_2[1]+3a_3[1]^2+4a_4[1]^3+6a_6[1]^5+\cdots+da_d[1]^{d-1}$$

$$=a_1+2a_2[1]+3a_3[1]+4a_4[1]+6a_6[1]+\cdots+da_d[1]+[0]$$

$$=a_1+a_2[2]+a_3[3]+a_4[4]+a_6[1]+a_7[2]+a_8[3]+a_9[4]+\cdots+da_d[1]$$

$$=A[1]+B[2]+C[3]+D[4]$$

dengan:

$A=(a_1+a_6+a_{11}+\cdots)$

$B=(a_2+a_7+a_{12}+\cdots)$

$C=(a_3+a_8+a_{13}+\cdots)$

$D=(a_4+a_9+a_{14}+\cdots)$

Keterangan: *A*, *B*, *C* , dan *D* adalah deret dengan batas da_d atau kurang dari da_d .

Misalnya, jika $da_d=a_{12}$ maka batas *A* adalah a_{11}, batas *B* adalah a_{12}, batas *C* adalah a_8, dan batas *D* adalah a_9.

Saat $x=[2](\mathrm{mod}\,5)$ maka

$$f'([2]) = a_1 + 2a_2[2] + 3a_3[2]^2 + 4a_4[2]^3 + 6a_6[2]^5 + \cdots + da_d[2]^{d-1}$$

$$= a_1 + 2a_2[2] + 3a_3[4] + 4a_4[3] + 6a_6[2] + \cdots + da_d[2]^{d-1}$$

$$= a_1 + 2a_2[2] + 3a_3[4] + 4a_4[3] + a_6[2] + 2a_7[4] + 3a_8[1] + 4a_9[2] + \cdots + da_d[2]^{d-1}$$

$$= a_1[1] + [2]a_2[2] + [3]a_3[4] + [4]a_4[3] + [1]a_6[2] + [2]a_7[4] + [3]a_8[1] + \cdots + da_d[2]^{d-1}$$

$$= E[1] + F[2] + G[3] + H[4]$$

dengan:

$$E = (a_1 + [2]a_6 + [4]a_{11} + [3]a_{16} + a_{21} + \cdots)$$

$$F = ([2]a_2 + [4]a_7 + [3]a_{12} + a_{17} + [2]a_{22} + \cdots)$$

$$G = ([4]a_3 + [3]a_8 + a_{13} + [2]a_{18} + [4]a_{23} + \cdots)$$

$$H = ([3]a_4 + a_9 + [2]a_{14} + [4]a_{19} + [3]a_{24} + \cdots)$$

Keterangan: *E, F, G, dan H* adalah deret dengan batas da_d atau kurang dari da_d.

Misalnya, jika $da_d = [4]a_{19}$ maka batas E adalah $[3]a_{16}$, batas F adalah a_{17}, batas G adalah $[2]a_{18}$, dan batas H adalah $[4]a_{19}$.

Saat $x = [3] (\mathrm{mod}\, 5)$ maka

$$f'([3]) = a_1 + 2a_2[3] + 3a_3[3]^2 + 4a_4[3]^3 + 6a_6[3]^5 + \cdots + da_d[3]^{d-1}$$

$$= a_1 + 2a_2[3] + 3a_3[4] + 4a_4[2] + 6a_6[3] + \cdots + da_d[3]^{d-1}$$

$$= a_1[1] + [3]a_6[1] + [2]a_2[3] + [2]a_7[4] + [3]a_2[3] + [3]a_7[4] + [4]a_4[2] + \cdots + da_d[3]^{d-1}$$

$$= I[1] + J[2] + K[3] + L[4]$$

dengan:

$$I = \left(a_1 + [3]a_6 + [4]a_{11} + [2]a_{16} + a_{21} + \cdots\right)$$

$$J = \left([3]a_2 + [4]a_7 + [2]a_{12} + a_{17} + [3]a_{22} + \cdots\right)$$

$$K = \left([4]a_3 + [2]a_8 + a_{13} + [3]a_{18} + [4]a_{23} + \cdots\right)$$

$$L = \left([2]a_4 + a_9 + [3]a_{14} + [4]a_{19} + [2]a_{24} + \cdots\right)$$

Keterangan: *I, J, K, dan L* adalah deret dengan batas da_d atau kurang dari da_d.

Misalnya, jika $da_d = [2]a_{24}$ maka batas *I* adalah a_{21}, batas *J* adalah $[3]a_{22}$, batas *K* adalah $[4]a_{23}$, dan batas *L* adalah $[2]a_{24}$.

Saat $x = [4] \pmod 5$ maka

$$\begin{aligned} f'([4]) &= a_1 + 2a_2[4] + 3a_3[4]^2 + 4a_4[4]^3 + 6a_6[4]^5 + \cdots + da_d[4]^{d-1} \\ &= a_1 + 2a_2[4] + 3a_3[1] + 4a_4[4] + 6a_6[1] + 7a_7[4] + 8a_8[1] + \cdots + da_d[4]^{d-1} \\ &= [1]a_1 + [2]a_2[4] + [3]a_3[1] + [4]a_4[4] + [1]a_6[4] + [2]a_7[1] + [3]a_8[4] + \cdots + da_d[4]^{d-1} \\ &= P[1] + Q[2] + R[3] + S[4] \end{aligned}$$

dengan:

$$P = \left(a_1 + [4]a_6 + a_{11} + [4]a_{16} + a_{21} + \cdots\right)$$

$$Q = \left([4]a_2 + a_7 + [4]a_{12} + a_{17} + [4]a_{22} + \cdots\right)$$

$$R = \left(a_3 + [4]a_8 + a_{13} + [4]a_{18} + a_{23} + \cdots\right)$$

$$S = \left([4]a_4 + a_9 + [4]a_{14} + a_{19} + [4]a_{24} + \cdots\right)$$

Keterangan: *P, Q, R, dan S* adalah deret dengan batas da_d atau kurang dari da_d.

Misalnya, jika $da_d = [4]a_{24}$ maka batas *P* adalah a_{21}, batas *Q* adalah $[4]a_{22}$, batas *R* adalah a_{23}, dan batas *S* adalah $[4]a_{24}$.

Karena $f'(x) \not\equiv 0 \pmod 5$ maka:

$$f'([0]) \not\equiv 0 \pmod 5 \Rightarrow a_1 \not\equiv 0 \pmod 5$$

$$f'([1]) \not\equiv 0 \pmod 5 \Rightarrow (A[1]+B[2]+C[3]+D[4]) \not\equiv 0 \pmod 5$$

$$f'([2]) \not\equiv 0 \pmod 5 \Rightarrow (E[1]+F[2]+G[3]+H[4]) \not\equiv 0 \pmod 5$$

$$f'([3]) \not\equiv 0 \pmod 5 \Rightarrow (I[1]+J[2]+K[3]+L[4]) \not\equiv 0 \pmod 5$$

$$f'([4]) \not\equiv 0 \pmod 5 \Rightarrow (P[1]+Q[2]+R[3]+S[4]) \not\equiv 0 \pmod 5$$

Dari ciri-ciri tersebut, maka diperoleh teorema sebagai berikut:

Teorema 3.6

Polinom $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ dengan $a_0, a_1, \ldots, a_d \in \mathbb{Z}$ maka $f(x)$ **PP** modulo 5^n, jika dan hanya jika $\forall d = 4m,\ m \geq 1$ memenuhi:

a. $a_1 \not\equiv 0 \pmod 5$,

b. $(a_4 + a_8 + a_{12} + \cdots + a_d) \equiv 0 \pmod 5$,

c. $(a_2 + a_6 + \cdots + a_{d-2})^2 \equiv 3(a_1 + a_5 + \cdots + a_{d-3})(a_3 + a_7 + \cdots + a_{d-1})$,

d. $(A[1]+B[2]+C[3]+D[4]) \not\equiv 0 \pmod 5$,

e. $(E[1]+F[2]+G[3]+H[4]) \not\equiv 0 \pmod 5$,

f. $(I[1]+J[2]+K[3]+L[4]) \not\equiv 0 \pmod 5$, dan

g. $\left(P[1]+Q[2]+R[3]+S[4]\right)\not\equiv 0(\mathrm{mod}\,5)$.

dengan:

$A=\left(a_1+a_6+a_{11}+\cdots\right),$

$B=\left(a_2+a_7+a_{12}+\cdots\right),$

$C=\left(a_3+a_8+a_{13}+\cdots\right),$

$D=\left(a_4+a_9+a_{14}+\cdots\right),$

$E=\left(a_1+[2]a_6+[4]a_{11}+[3]a_{16}+a_{21}+\cdots\right),$

$F=\left([2]a_2+[4]a_7+[3]a_{12}+a_{17}+[2]a_{22}+\cdots\right),$

$G=\left([4]a_3+[3]a_8+a_{13}+[2]a_{18}+[4]a_{23}+\cdots\right),$

$H=\left([3]a_4+a_9+[2]a_{14}+[4]a_{19}+[3]a_{24}+\cdots\right),$

$I=\left(a_1+[3]a_6+[4]a_{11}+[2]a_{16}+a_{21}+\cdots\right),$

$J=\left([3]a_2+[4]a_7+[2]a_{12}+a_{17}+[3]a_{22}+\cdots\right),$

$K=\left([4]a_3+[2]a_8+a_{13}+[3]a_{18}+[4]a_{23}+\cdots\right),$

$L=\left([2]a_4+a_9+[3]a_{14}+[4]a_{19}+[2]a_{24}+\cdots\right),$

$P=\left(a_1+[4]a_6+a_{11}+[4]a_{16}+a_{21}+\cdots\right),$

$Q=\left([4]a_2+a_7+[4]a_{12}+a_{17}+[4]a_{22}+\cdots\right),$

$R=\left(a_3+[4]a_8+a_{13}+[4]a_{18}+a_{23}+\cdots\right),$

$S=\left([4]a_4+a_9+[4]a_{14}+a_{19}+[4]a_{24}+\cdots\right)$, dan batas *A*-*S* adalah da_d atau kurang dari da_d (Singh dan Maity, 2005:5).

Bukti:

$(\Rightarrow)$

Misalkan polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan koefisien-koefisiennya bilangan bulat $(a_0,a_1,\ldots,a_d\in\mathbb{Z})$. Menurut akibat 2.1 $f(x)$ PP modulo $5^n, n>1$ jika dan hanya jika $f(x)$ PP modulo 5 dan $f'(x)\not\equiv 0(\text{mod}\,5)$, untuk setiap x unsur di modulo 5.

Karena $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$, maka

$$f'(x)=a_1+2a_2x+3a_3x^2+4a_4x^3+\cdots+da_dx^{d-1}$$

$$=a_1+2a_2x+3a_3x^2+4a_4x^3+6a_6x^5+\cdots+da_dx^{d-1}+[0]$$

Saat $x=[0](\text{mod}\,5)$ maka

$$f'([0])=a_1+2a_2[0]+3a_3[0]^2+4a_4[0]^3+6a_6[0]^5+\cdots+da_d[0]^{d-1}+[0]$$

$$=a_1+[0]$$

Saat $x=[1](\text{mod}\,5)$ maka

$$f'([1])=a_1+2a_2[1]+3a_3[1]^2+4a_4[1]^3+6a_6[1]^5+\cdots+da_d[1]^{d-1}$$

$$=a_1+2a_2[1]+3a_3[1]+4a_4[1]+6a_6[1]+\cdots+da_d[1]+[0]$$

$$=a_1+a_2[2]+a_3[3]+a_4[4]+a_6[1]+a_7[2]+a_8[3]+a_9[4]+\cdots+da_d[1]$$

$$=A[1]+B[2]+C[3]+D[4]$$

Saat $x=[2](\text{mod}\,5)$ maka

$$f'([2]) = a_1 + 2a_2[2] + 3a_3[2]^2 + 4a_4[2]^3 + 6a_6[2]^5 + \cdots + da_d[2]^{d-1}$$

$$= a_1 + 2a_2[2] + 3a_3[4] + 4a_4[3] + 6a_6[2] + \cdots + da_d[2]^{d-1}$$

$$= a_1 + 2a_2[2] + 3a_3[4] + 4a_4[3] + a_6[2] + 2a_7[4] + 3a_8[1] + 4a_9[2] + \cdots + da_d[2]^{d-1}$$

$$= a_1[1] + [2]a_2[2] + [3]a_3[4] + [4]a_4[3] + [1]a_6[2] + [2]a_7[4] + [3]a_8[1] + \cdots + da_d[2]^{d-1}$$

$$= [1]a_1 + [2]a_6[1] + [2]a_2[2] + [2]a_7[4] + [3]a_3[4] + [3]a_8[1] + [4]a_4[3] + \cdots + da_d[2]^{d-1}$$

$$= E[1] + F[2] + G[3] + H[4]$$

Saat $x=[3](\text{mod}\,5)$ maka

$$f'([3]) = a_1 + 2a_2[3] + 3a_3[3]^2 + 4a_4[3]^3 + 6a_6[3]^5 + \cdots + da_d[3]^{d-1}$$

$$= a_1 + 2a_2[3] + 3a_3[4] + 4a_4[2] + 6a_6[3] + \cdots + da_d[3]^{d-1}$$

$$= a_1[1] + [3]a_6[1] + [2]a_2[3] + [2]a_7[4] + [3]a_2[3] + [3]a_7[4] + [4]a_4[2] + [4]a_9 + \cdots + da_d[3]^{d}$$

$$= I[1] + J[2] + K[3] + L[4]$$

Saat $x=[4](\text{mod}\,5)$ maka

$$f'([4]) = a_1 + 2a_2[4] + 3a_3[4]^2 + 4a_4[4]^3 + 6a_6[4]^5 + \cdots + da_d[4]^{d-1}$$

$$= a_1 + 2a_2[4] + 3a_3[1] + 4a_4[4] + 6a_6[1] + 7a_7[4] + 8a_8[1] + \cdots + da_d[4]^{d-1}$$

$$= [1]a_1 + [2]a_2[4] + [3]a_3[1] + [4]a_4[4] + [1]a_6[4] + [2]a_7[1] + [3]a_8[4] + \cdots + da_d[4]^{d-1}$$

$$= P[1] + Q[2] + R[3] + S[4]$$

Karena $f'(x) \not\equiv 0 \pmod 5, \forall x \in M_5$ maka $f'([0]), f'([1]), f'([2]), f'([3]),$ dan $f'([4])$ tidak kongruen dengan $0 \pmod 5$. Sehingga dari hasil ini dan sesuai dengan teorema 3.5 maka diperoleh sifat-sifat dari poin a sampai g.

$(\Leftarrow)$

Diberikan $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$ dengan ciri koefisiennya sesuai poin a sampai g pada teorema 3.6. Maka sesuai dengan teorema 3.5 $f(x)$ adalah PP modulo 5. Selanjutnya akan dibuktikan bahwa $f'(x) \not\equiv 0 \pmod 5, \forall x \in \mathbb{Z}_5$.

Saat $x = [0] \pmod 5$ maka:

$$f'([0]) = a_1 + 2a_2[0] + 3a_3[0]^2 + 4a_4[0]^3 + 6a_6[0]^5 + \cdots + da_d[0]^{d-1}$$

$$= a_1 + [0]$$

Karena $a_1 \not\equiv 0 \pmod 5$ maka $f([0]) \not\equiv 0 \pmod 5$.

Saat $x = [1] \pmod 5$ maka:

$$f'([1]) = A[1] + B[2] + C[3] + D[4]$$

Karena $A[1] + B[2] + C[3] + D[4] \not\equiv 0 \pmod 5$ maka $f([1]) \not\equiv 0 \pmod 5$.

Saat $x = [2] \pmod 5$

$$f'([2]) = E[1] + F[2] + G[3] + H[4]$$

Karena $E[1] + F[2] + G[3] + H[4] \not\equiv 0 \pmod 5$, maka $f([2]) \not\equiv 0 \pmod 5$.

Saat $x=[3](\mathrm{mod}\,5)$

$$f'([3])=I[1]+J[2]+K[3]+L[4]$$

Karena $I[1]+J[2]+K[3]+L[4]\not\equiv 0(\mathrm{mod}\,5)$, maka $f([3])\not\equiv 0(\mathrm{mod}\,5)$.

Saat $x=[4](\mathrm{mod}\,5)$ maka

$$f'([4])=P[1]+Q[2]+R[3]+S[4]$$

Karena $P[1]+Q[2]+R[3]+S[4]\not\equiv 0(\mathrm{mod}\,5)$, maka $f([3])\not\equiv 0(\mathrm{mod}\,5)$

Karena terbukti bahwa $f(x)$ PP modulo 5 dan $f'(x)\neq[0](\mathrm{mod}\,5)$ sesuai dengan akibat 2.1 maka $f(x)$ PP modulo 5^n.

Contoh 3.7

Misalkan $q(x)=x^5+x^3+4x^2+x+3$. Pemetaan modulo 25 atau (5^2) oleh $q(x)$ adalah sebagai berikut:

$q:[0]\to[3]$	$q:[1]\to[10]$	$q:[2]\to[11]$	$q:[3]\to[12]$
$q:[4]\to[9]$	$q:[5]\to[8]$	$q:[6]\to[20]$	$q:[7]\to[6]$
$q:[8]\to[22]$	$q:[9]\to[14]$	$q:[10]\to[13]$	$q:[11]\to[5]$
$q:[12]\to[1]$	$q:[13]\to[7]$	$q:[14]\to[19]$	$q:[15]\to[18]$
$q:[16]\to[15]$	$q:[17]\to[21]$	$q:[18]\to[17]$	$q:[19]\to[24]$
$q:[20]\to[23]$	$q:[21]\to[0]$	$q:[22]\to[16]$	$q:[23]\to[2]$
$q:[24]\to[4]$			

Pemetaan diatas membentuk permutasi yaitu:

$$([0][3][12][1][10][13][7][6][20][23][2][11][5][8][22][16][15][18][17][21])$$

$$([4][9][14][19][24]).$$

3.5 Polinomial Permutasi dalam Pandangan Islam

Polinomial permutasi terdiri dari dua kata, yaitu polinomial dan permutasi. Polinom atau suku banyak memiliki derajat pada masing-masing sukunya dan masing-masing suku disambungkan dengan operasi penjumlahan. Jika kita lihat bentuk umum dari polinom seperti berikut ini:

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d + \cdots$$

dengan x variabel tak tentu dan a_i koefisien dari masing-masing suku x^i untuk setiap i mulai dari 0 sampai tak hingga. Dari bentuk umum polinom ini kita umpamakan sebagai sebuah komunitas di mana x sebagai masing-masing individu. Derajat (pangkat) dari setiap suku menunjukkan derajat masing-masing individu, semakin tinggi derajat seseorang maka akan semakin dekat dengan suku tertinggi (yang memiliki derajat tertinggi) dengan derajat tak hingga yaitu Allah SWT. Sudah pasti individu yang paling dekat dengan Allah adalah Nabi Muhammad SAW kemudian disusul dengan para nabi dan rasul-Nya, para malaikat, sahabat-sahabat nabi, dan seterusnya semua memiliki derajat masing-masing sesuai dengan tingkat ketaqwaannya kepada Allah. Jika seorang hamba tidak mau patuh dan taat kepada Allah maka derajatnya pun sangat rendah dihadapan Allah dan pada polinom ditunjukkan (diibaratkan) dengan suku pertamanya yaitu a_0. a_0 secara matematis memiliki derajat nol karena $x^0 = 1$.

Jadi seseorang yang tidak patuh dan taat kepada Allah seolah–olah tidak memiliki derajat (tidak dianggap) dihadapan-Nya. Mengenai derajat Allah juga berfirman dalam penggalan Surat Al-Mu'min ayat 15 yang artinya:

"(Dialah) Yang Maha Tinggi derajat-Nya, Yang mempunyai 'Arsy..."

Di lain hal hikmah juga diperoleh dari bentuk umum polinom. Misalkan dalam sebuah negara setiap individu mempunyai derajat (pangkat) masing-masing. Dari presiden yang memiliki pangkat tertinggi, hingga rakyat yang memiliki pangkat terendah. Operasi penjumlahan (+) menunjukkan bahwa semua elemen harus saling membantu, mendukung dan melaksanakan tugas masing-masing agar tercipta keharmonisan dan kedamaian di negaranya. Jika tidak saling melengkapi (seperti saling bermusuhan, melakukan pelanggaran hukum, atau pemberontakan misalnya) maka kedamaian dan ketentraman mungkin akan menjadi angan-angan belaka.

Sedangkan permutasi adalah pemetaan satu-satu dan onto (bijektif) dari himpunan berhingga pada dirinya sendiri. Definisi ini sejalan dengan kajian pustaka pada bab sebelumnya, dimana ayat ke-15 dalam Surat Al-Jatsiyah menjelaskan bahwa setiap amal perbuatan akan kembali kepada yang melakukannya. Jika kebaikan yang dilakukan maka kebaikan pula yang akan diperolehnya, begitu pula jika keburukan yang kerjakan maka keburukan juga yang didapatkan. Hal ini dapat kita buktikan dalam kehidupan sehari-hari. Jika kita berbuat baik kepada sesama pasti akan dibalas dengan kebaikan pula, seandainya tidak dibalas dengan kebaikan, atau malah tidak menghiraukan apa

yang telah kita lakukan, ini hanya semata ujian dari Allah, apakah kita mampu atau tidak melewati ujian tersebut.

Jika permutasi memetakan daerah asal kembali ke daerah asal, maka ayat ini memetakan amal perbuatan yang dilakukan kembali kepada pelakunya masing-masing. Kebaikan dipetakan atau dibalas dengan kebaikan, begitu juga keburukan dibalas dengan keburukan. Jadi dari ayat ini diperoleh dua hal sebagai berikut:

1. Amal perbuatan memetakan yang melakukan perbuatan tersebut kembali pada orang yang melakukannya maksudnya perbuatan yang dilakukan akibatnya tidak mungkin dilimpahkan kepada orang lain, pasti dikembalikan (balasannya) kepada dirinya sendiri.
2. Allah memetakan (membalas) perbuatan dengan perbuatan yang sama, maksudnya jika perbuatan baik dilakukan maka balasannya juga kebaikan (surga) sedangkan jika perbuatan buruk yang dikerjakan maka balasannya adalah keburukan (neraka).

Dari pembahasan polinom dan permutasi di atas, maka polinomial permutasi berarti polinom memetakan himpunan berhingga kembali ke himpunan itu sendiri. Hampir sama dengan definisi permutasi, hanya saja pemetaan yang digunakan adalah fungsi polinom. Tidak semua polinom pasti memetakan daerah asal kembali ke daerah tersebut, ada dua kemungkinan, yaitu:

1. Polinom tersebut memetakan ke himpunan lain. Ini tidak bertentangan dengan apa yang telah dibahas sebelumnya. Misalkan jika seseorang melakukan perbuatan baik belum tentu amal perbuatan itu dicatat oleh Allah sebagai amal kebaikan, namun sebaliknya. Hal ini diakibatkan banyak

faktor misalnya niat yang tidak ikhlas. Orang yang menyedekahkan sebagian hartanya, namun tidak dengan niat yang ikhlas semata karena Allah. Maka sedekah ini tidak memperoleh pahala dan sia-sia saja dihadapan Allah, atau bahkan Allah membenci orang tersebut jika niatnya hanya untuk pamer dan menyombongkan harta yang diamanahkan Allah kepada orang tersebut.

2. Ada juga yang pemetaan yang tidak bersifat bijektif (satu-satu dan onto). Dalam kasus modulo, peta dari polinom tidak mungkin keluar dari himpunan itu sendiri, namun bisa saja ada lebih dari satu unsur dipetakan ke satu unsur yang sama. Contohnya, Nabi Muhammad sebagai uswatun hasanah bagi umat islam pasti akan dijadikan rujukan bagi setiap muslim di dunia ini. Semua merujuk kepada beliau baik dalam hal duniawi maupun ukhrawi, karena beliau merupakan satu dari dua tutunan yang tidak akan menyesatkan kita sebagai umat muslim jika kita mengikuti sunnah-sunnah beliau. Jadi jika ada himpunan umat muslim dengan pemetaan didefinisikan dengan "panutan atau idola" maka setiap muslim pasti dipetakan kepada Nabi SAW.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan pada bab sebelumnya, penulis memberikan beberapa kesimpulan, di antaranya:

1. Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$ adalah Polinomial Permutasi (PP) pada:
   a. Modulo 2 jika dan hanya jika $(a_1+a_2+\cdots+a_d)$ bilangan bulat ganjil.
   b. Modulo 2^n, $n>1$ jika dan hanya jika a_1 bilangan bulat ganjil, $(a_2+a_4+a_6+\cdots+a_d)$ dan $(a_3+a_5+a_7+\cdots+a_{d-1})$ bilangan bulat genap.
2. Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$ adalah PP modulo 3 jika dan hanya jika $(a_1+a_3+a_5+\cdots)\not\equiv 0(\mathrm{mod}\,3)$ dan $(a_2+a_4+a_6+\cdots)\equiv 0(\mathrm{mod}\,3)$.
3. Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$ adalah PP modulo $3^n, n>1$ jika dan hanya jika
   a. $a_1\not\equiv 0(\mathrm{mod}\,3)$,
   b. $(a_1+a_3+a_5+\cdots)\not\equiv 0(\mathrm{mod}\,3)$,
   c. $(a_2+a_4+a_6+\cdots)\equiv 0(\mathrm{mod}\,3)$,

d. $T[1]+U[2]\not\equiv 0(\mathrm{mod}\,3)$, dan

e. $M[1]+N[2]\not\equiv 0(\mathrm{mod}\,3)$.

dengan:

$T=(a_1+a_4+a_7+a_{10}+\cdots)$,

$U=2(a_2+a_5+a_8+a_{11}+\cdots)$,

$M=(a_1+a_2+a_7+a_8+\cdots)$, dan

$N=(a_4+a_5+a_{10}+a_{11}+\cdots)$.

Keterangan: Poin b sampai e merupakan deret dengan batas da_d atau kurang dari da_d.

4. Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$ adalah PP modulo 5, jika dan hanya jika $\forall d=4m,\ m\geq 1$, memenuhi:

a. $(a_2+a_6+\cdots+a_{d-2})^2\equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$, dan

b. $(a_4+a_8+\cdots+a_d)\equiv 0(\mathrm{mod}\,5)$.

5. Polinom $f(x)=a_0+a_1x+a_2x^2+\cdots+a_dx^d$ dengan $a_0,a_1,\ldots,a_d\in\mathbb{Z}$ adalah PP modulo 5^n, jika dan hanya jika $\forall d=4m,\ m\geq 1$, memenuhi:

a. $a_1\not\equiv 0(\mathrm{mod}\,5)$,

b. $(a_4+a_8+a_{12}+\cdots+a_d)\equiv 0(\mathrm{mod}\,5)$,

c. $(a_2+a_6+\cdots+a_{d-2})^2\equiv 3(a_1+a_5+\cdots+a_{d-3})(a_3+a_7+\cdots+a_{d-1})$,

d. $(A[1]+B[2]+C[3]+D[4])\not\equiv 0(\mathrm{mod}\,5)$,

e. $\left(E[1]+F[2]+G[3]+H[4]\right)\not\equiv 0(\mathrm{mod}\,5)$,

f. $\left(I[1]+J[2]+K[3]+L[4]\right)\not\equiv 0(\mathrm{mod}\,5)$, dan

g. $\left(P[1]+Q[2]+R[3]+S[4]\right)\not\equiv 0(\mathrm{mod}\,5)$.

dengan:

$A=\left(a_1+a_6+a_{11}+\cdots\right)$,

$B=\left(a_2+a_7+a_{12}+\cdots\right)$,

$C=\left(a_3+a_8+a_{13}+\cdots\right)$,

$D=\left(a_4+a_9+a_{14}+\cdots\right)$,

$E=\left(a_1+[2]a_6+[4]a_{11}+[3]a_{16}+a_{21}+\cdots\right)$,

$F=\left([2]a_2+[4]a_7+[3]a_{12}+a_{17}+[2]a_{22}+\cdots\right)$,

$G=\left([4]a_3+[3]a_8+a_{13}+[2]a_{18}+[4]a_{23}+\cdots\right)$,

$H=\left([3]a_4+a_9+[2]a_{14}+[4]a_{19}+[3]a_{24}+\cdots\right)$,

$I=\left(a_1+[3]a_6+[4]a_{11}+[2]a_{16}+a_{21}+\cdots\right)$,

$J=\left([3]a_2+[4]a_7+[2]a_{12}+a_{17}+[3]a_{22}+\cdots\right)$,

$K=\left([4]a_3+[2]a_8+a_{13}+[3]a_{18}+[4]a_{23}+\cdots\right)$,

$L=\left([2]a_4+a_9+[3]a_{14}+[4]a_{19}+[2]a_{24}+\cdots\right)$,

$P=\left(a_1+[4]a_6+a_{11}+[4]a_{16}+a_{21}+\cdots\right)$,

$Q=\left([4]a_2+a_7+[4]a_{12}+a_{17}+[4]a_{22}+\cdots\right)$,

$R = \left(a_3 + [4]a_8 + a_{13} + [4]a_{18} + a_{23} + \cdots\right)$,

$S = \left([4]a_4 + a_9 + [4]a_{14} + a_{19} + [4]a_{24} + \cdots\right)$, dan batas A-S adalah da_d atau kurang dari da_d.

4.2 Saran

Penulis menyarankan dua poin yang dapat digunakan untuk penelitian selanjutnya, yaitu:

1. Sifat-sifat polinomial permutasi pada modulo 7^n, 11^n, dan seterusnya.
2. Sifat-sifat umum polinomial permutasi modulo p^n.

DAFTAR PUSTAKA

Abdussakir. 2007. *Ketika Kyai Mengajar Matematika*. Malang: UIN Maliki Press.

Al-Jazairi, S.A.B.J.. 2009. *Tafsir Al-Qur'an Al-Aisar*, Jilid 6. Jakarta: Darus Sunnah.

Fraleigh, V.J.K.. 2004. *A First Course in Abstract Algebra*. Boston: Addison-Wesley Publishing Company.

Hardy, G. H. dan Wright, E.M.. 2009. *An Introduction to The Theory of Number, Sixth Edition*. Oxford: Post and Telecom Press.

Lidl, R. dan Niederreiter, H.. 1997. *Finite Fields*. Cambridge: Cambridge University Press.

Mollin, R.A. dan Small, C.. 1987. *On Permutation Polynomials over Finite Fields*. Calgary: University of Calgary Press.

Raisinghania, M.D. dan Anggarwal, R.S.. 1980. *Modern Algebra*. New Delhi: S.Chand & Company LTD.

Shallue, J.C.. 2012. *Permutation of Finite Fields*. Monash: Monash University Press.

Singh, R.P. dan Maity, S.. 2009. *Permutation Polynomials Modulo* p^n. Nevada: IACR Press.

Thabathaba'i, M.H.. 2005. *Ada Apa Setelah Mati? Pandangan Al-Qur'an*. Jakarta: Penerbit Misbah.